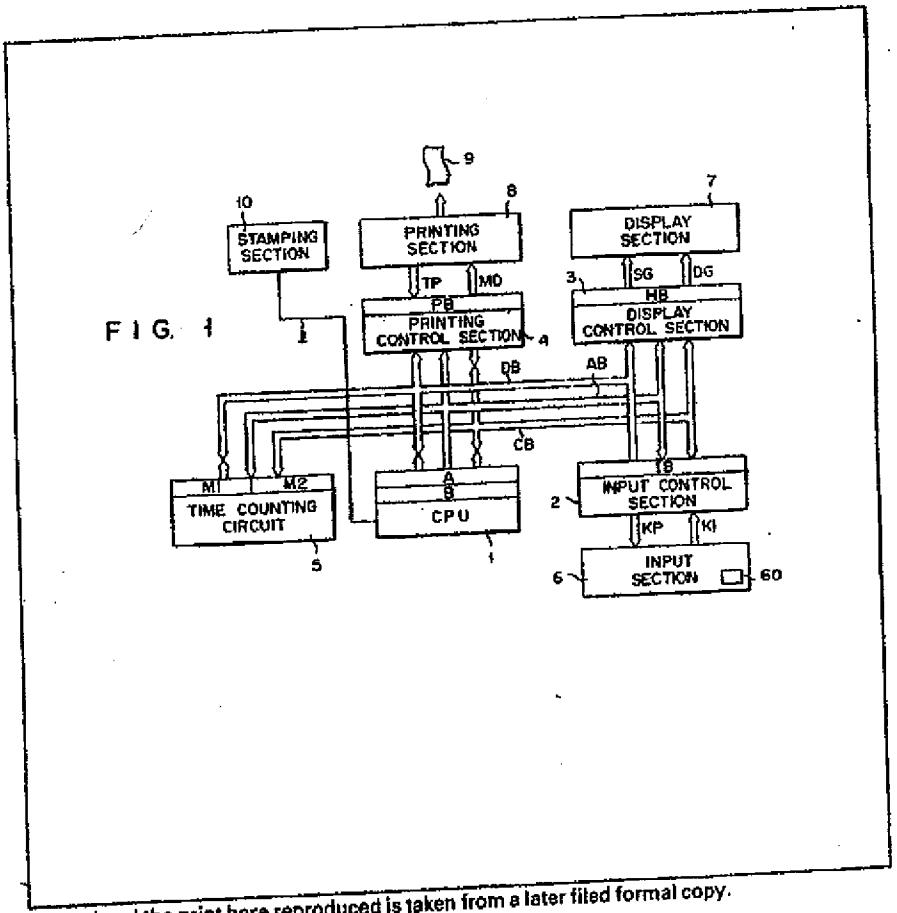
(12) UK Patent Application (19) GB (11) 2 065 030 A

(21) Application No 8038192
(22) Date of filing 28 Nov 1980
(30) Priority data
(31) 54/155823
(32) 30 Nov 1979
(33) Japan (JP)
(43) Application published
24 Jun 1981
(51) INT CL³
G07C 1/04
(52) Domestic classification
B6A DX
(56) Documents cited
GB 1259091
(58) Field of search
B6A
B6C
B6F
G4T

(71) Applicants
Casio Computer Co., Ltd.,
6-1, 2-chome,
Nishi-Shinjuku,
Shinjuku-ku,
Tokyo,
Japan.
(72) Inventors
Seiichi Shibata
(74) Agents
A. A. Thornton & Co.,
Northumberland House,
303/306 High Holborn,
London, WC1V 7LE.

(54) **Note-paper sheet issuance device**

(57) In a small-sized electronic apparatus having at least a time counting circuit (5) and a printing section (8), when a note-paper sheet issuance key (6a) is operated a note-paper sheet, on which the present time data is printed and also which has a blank space for receiving messages, is issued. The apparatus is particularly suited for taking memoranda of telephone calls.



F I G. 1

GB 2 065 030 A

The drawings originally filed were informal and the print here reproduced is taken from a later filed formal copy.

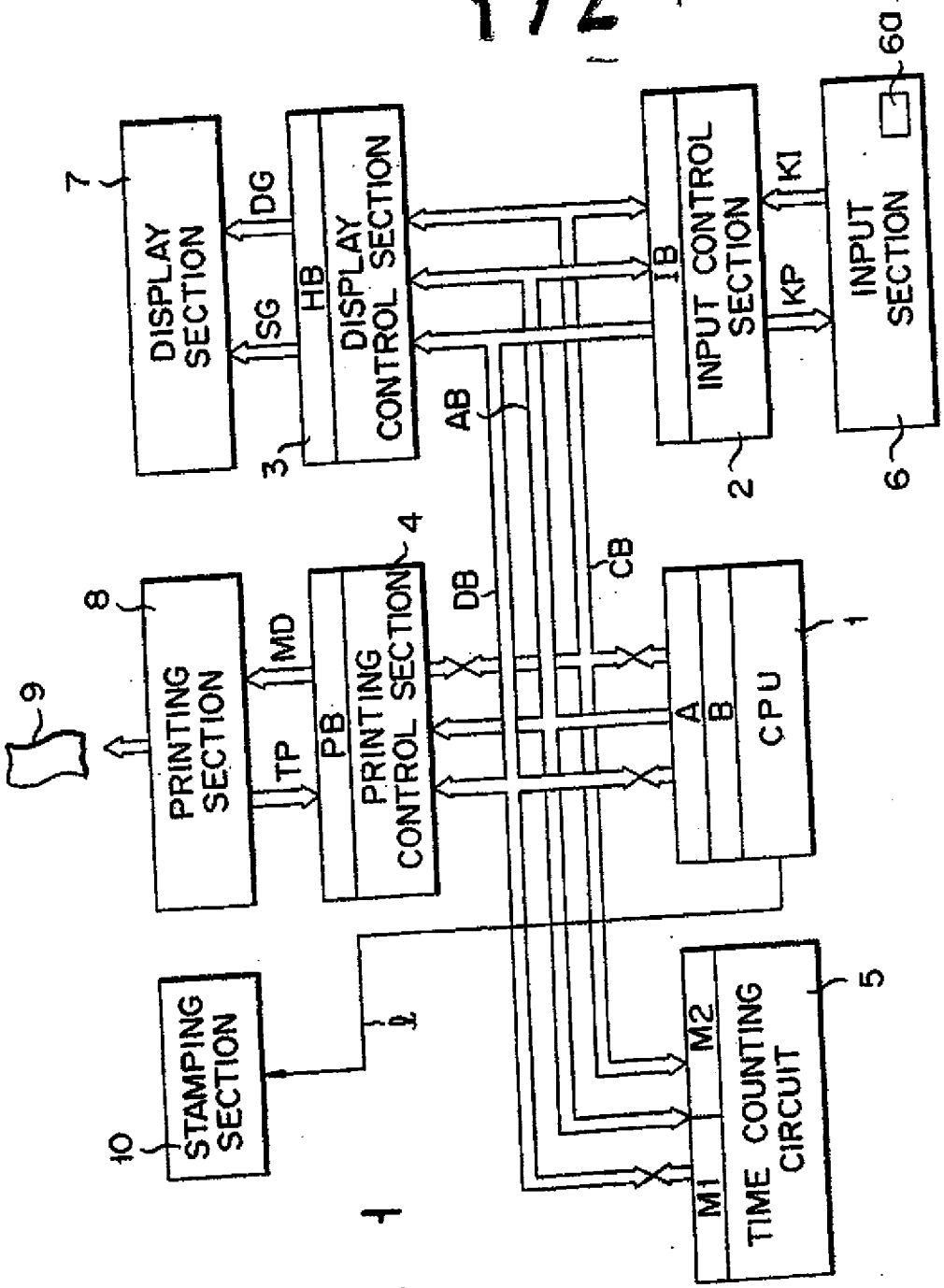

DISPLAY SECTION
7
DG
SG
HB
DISPLAY CONTROL SECTION
3
AB
IB
INPUT CONTROL SECTION
2
KI
KP
INPUT SECTION
6a
6
PRINTING SECTION
8
MD
TP
PB
PRINTING CONTROL SECTION
4
DB
CB
A
B
CPU
1
9
STAMPING SECTION
10
M2
M1
TIME COUNTING CIRCUIT
5

FIG. 1

FIG. 2

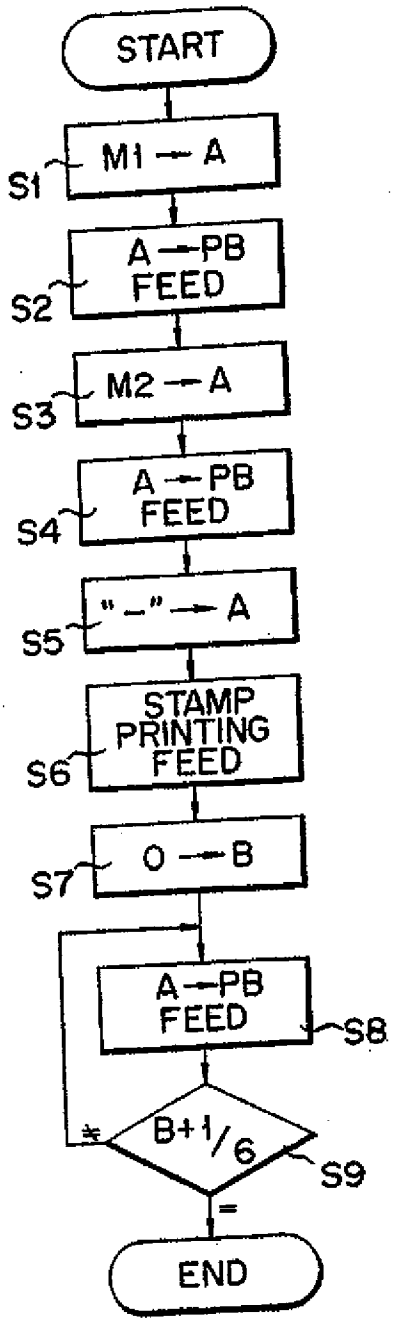


FIG. 3

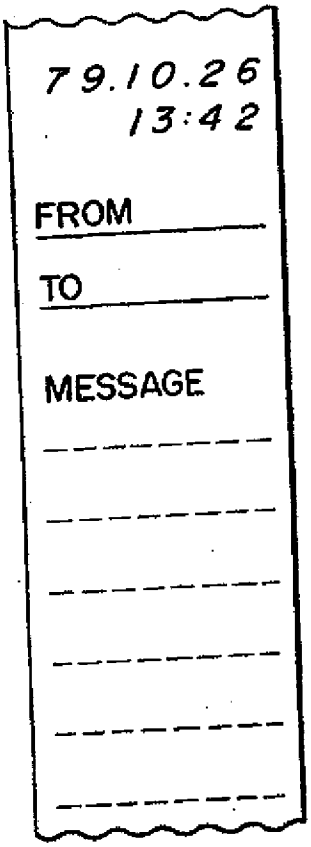
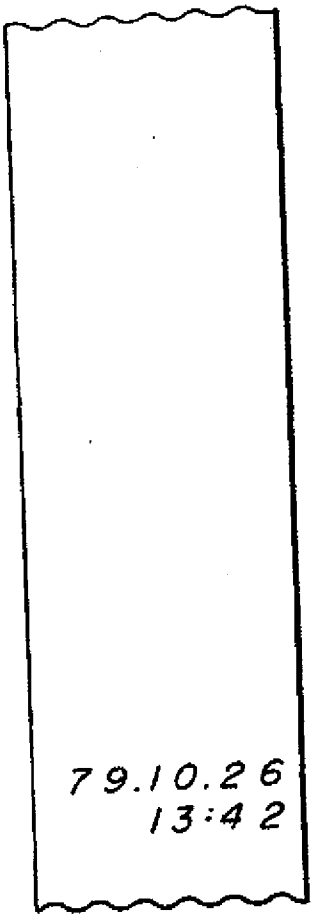


FIG. 4



SPECIFICATION

Note-paper sheet issuance device

In our daily life, there often occurs an occasion when one responds to a telephone call addressed to an absent person and writes a message of the calling person on note-paper. When writing such a message, it is usual to also write the time data of the instant of reception of the call on the same note-paper. However, it is quite often the case to neglect or forget to write the time data of the instant of reception of the message. In such a case, the value of the message as such is sometimes reduced. In addition, it sometimes takes time to find out a note-paper sheet on which to write a message, and also without any definite format of the note-paper some wasteful time is involved when reading the written message.

An object of the invention is to provide an apparatus which can automatically issue a note-paper sheet, on which the present time data is printed and also which has a blank space for writing a message or the like therein, in response to the operation of a note-paper sheet issuance key.

To achieve the above object, the note-paper sheet issuing apparatus according to the invention comprises a keying section having a note-paper issuance key, a central processing unit connected to the keying section, a time counting circuit connected to the central processing unit for automatically renewing the present time data such as present hour and minute data, and a printing section connected to the central processing unit and serving to print the present time data at the time when the note-paper sheet issuance key is operated and also feeding the sheet by a predetermined interval for providing a blank space before the start of or after the end of the printing operation.

With the above construction, it is possible to provide a note-paper sheet with the present time data printed thereon by one-touch keying operation. Thus, when the invention is applied to a table telephone set with printer, in case of taking memo of a telephone message a note-paper sheet with the present time data printed therein and having a blank space for writing the message can be obtained from the table telephone set on a desk by one-touch keying operation, and this is very convenient. In addition, the time for writing the time data of the instant of reception of the message can be saved, and also there is no possibility of neglecting the writing of the time data. Further, since the note-paper sheet has a definite formula, the content written on the sheet can be readily read out.

This invention can be more fully understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

Figure 1 is a block diagram showing a printing calculator;

Figure 2 is a flow chart illustrating the operation of a note-paper sheet issuing apparatus; and

Figures 3 and *4* show examples of the format of note-paper sheet.

Now, an embodiment of the invention will be described with reference to Figures 1 through 4. Figure 1 outlines the construction of a printing calculator. In the Figure, designated at 1 is a central processing unit (CPU). The CPU 1 includes a control section, in which various microcommands are stored, and an arithmetic section for effecting summing and subtracting operations. It also includes various registers such as A and B registers for temporarily memorizing data at the time of display, printing, transfer and arithmetic processing of data. An input control section 2, a display control section 3, a printing control section 4 and a time counting circuit 5 are connected to the CPU 1 through a data bus DB, an address bus AB and a control bus CB. The input control section 2 includes an input buffer IB for temporarily memorizing input data. This input control section 2 is providing a timing signal KP to an input section 6, and when keying operation is done in the input section 6 the timing signal is selectively fed as a keyed input signal to the input buffer memory IB of the input control section 2 according to the operated key. The input section 6 is provided with ten keys for coupling numerical values "0" to "9" and function keys for coupling arithmetic instructions as well as a note-paper issuing key 6a which is operated when issuing a note-paper sheet.

The display control section 3 includes a display buffer HB, and segment signal SG obtained as a result of decoding of display data in the display buffer HB is supplied together with digit signal DG to a display section 7. In the display section 7, numeral data or the like are digitally displayed according to the input signal.

The printing control section 4 includes a printing buffer PB for detecting the coincidence of printing data in the printing buffer 4 and printing position signal TP transferred from a printing section 8, and the result of the detection is supplied as printing drive signal MD to the printing section 8. In the printing section 8, given hammers are driven according to the printing drive signal MD, thus producing a sheet 9, on which numeral data and the like are printed.

The time counting circuit 5 includes a data information memory section M_1 for memorizing the data information of the present data, namely year, month and day data thereof, and a time information memory section M_2 for memorizing the time information of the present time, namely hour and minute data thereof. The data memorized in the memory section M_1 and M_2 are automatically renewed in accordance with the time counting operation performd within the time counting circuit 5.

Designated at 10 is a stamping section. In this section, impressions "From _____", "To _____" and "Content of message" are stamped when a stamp drive command is given from the CPU 1 through a line ℓ.

The operation of the table telephone set with printer of the above construction for issuing a note-paper sheet will now be described. When a call to an absent person is received and it is necessary to write a message of the calling person on a note-paper sheet, the note-paper sheet issuance key 6a is

operated. As a result, operation as shown by the flow chart of Figure 2 is executed. In a first S_1, the present data information, i.e., present year, month and day data, memorized in the data information memory section M_1 of the time counting circuit 5 are read out and written in the A register in the CPU 1. In the next step S_2, the date data written in the A register is transferred to the printing buffer PB in the printing control section 4, and the present date information is recorded on a recording sheet according to printing drive signal MD corresponding to the data in the printing buffer PB and supplied to the printing section 8. Subsequently, the sheet is fed by one line interval. In this step, the present date information, for instance "79.10.26", is printed as shown in Figure 2. In the following step S_3, the present time information, i.e., present hour and minute data, memorized in the time information memory section M_2 are read out and written in the A register. In the following step S_4, the time data in the A register is transferred to the printing buffer PB, and the present time is printed in the printing section 8. Subsequently, the sheet is fed by one line interval. In this step, the present time information, for instance "13:42", is printed. In the following step S_5, a bar code "–" is written in the A register. In the following step S_6, a stamp drive command is produced from the CPU 1 and coupled through the line to the stamping section 10, an impression of an underlined space "From ———", in which to write the surname of the caller, an impression of an underlined space "To ———", in which to write the surname of the called, and an impression "Content of message" are stamped. At this time, the sheet is fed by one line interval after each impression is stamped. In the following step S_7, "0" is written in the B register of CPU 1. In the following step S_8, the bar code written in the A register is transferred to the printing buffer PB, and bar codes for one line are printed in the A register. Subsequently, the sheet is fed by one line interval. In the following step S_9, the sum of the content of the B register and "1" is taken and written as new content in the B register, and whether or not the new content is equal to "6", that is, whether or not printing of bar codes for 6 lines has been effected, is checked. If the check yields "yes", the operation of producing a note-paper sheet is ended. If the check yields "no", the operation returns to the step S_8 of printing bar codes.

In the above way, by operating the note-paper sheet issuance key 6a once, a note-paper sheet, on which the present data and time data are printed as shown in Figure 3, and the person who has received the call can write surnames of the calling and called persons in the predetermined spaces.

Figure 4 shows a difference example of the format of the note-paper sheet which is issued when the note-paper sheet issuance key 6a is operated. In this embodiment, with the operation of the key 6a a sheet is fed to a predetermined extent, and then the data and time data are printed after the blank space thus provided.

It is further possible to adopt various other formats of the note-paper sheet. For example, instead of the format shown in Figure 3, a blank space may be provided by feeding the sheet by a predetermined interval after the printing of the data and time data. Also, instead of the blank space in the format shown in Figure 4, the aforementioned stamped impressions of the characters and bar codes may be given.

Further, the content of the stamped impressions in the format of Figure 3 is by no means limitative, and various stamped impression may be provided depending upon use.

CLAIMS

1. An apparatus for issuing note-paper sheets comprising:

a keying section having a note-paper sheet issuance key;

a central processing unit connected to said keying section;

a time counting circuit connected to said central processing unit for automatically renewing the present time data such as present hour and minute data; and

a printing section connected to said central processing unit and serving to print said present time data on a paper sheet at the time and also feeding said sheet by a predetermined interval for providing a blank space before the start of or after the end of the printing operation at the time when said note-paper sheet issuance key is operated.

2. An apparatus according to Claim 1, wherein:

said time counting circuit automatically renews present date and time data consisting of present date data and present time and minute data; and

said printing section prints said present date and time data at the time and also feeds the recording sheet for providing a blank space before the start of or after the end of the printing operation at the time when said note-paper sheet issuance key is operated.

3. An apparatus according to Claim 1, wherein said printing section prints said present time data at the time when said note-paper sheet issuance key is operated and also prints bar codes spaced apart at predetermined interval before the start of or after the end of the printing operation.

4. An apparatus according to Claim 1, which further comprises a stamping section connected to said central processing unit for providing stamped impressions on the recording sheet emerging from said printing section.

5. An apparatus according to Claim 1, wherein:

said keying section has ten keys and function keys for supplying arithmetic commands for addition, subtraction, multiplication and division:

said central processing unit executes calculating operation; and

said printing section prints numeral data and data of the result of calculation.

6. A note-paper sheet issuance device, substantially as hereinbefore described with reference to the accompanying drawings.

Printed for Her Majesty's Stationery Office by Croydon Printing Company Limited, Croydon, Surrey, 1981.
Published by The Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 132 782
A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 84108486.6

(22) Date of filing: 18.07.84

(51) Int. Cl.⁴: G 07 B 17/02

(30) Priority: 18.07.83 US 515086
21.07.83 US 515760

(43) Date of publication of application:
13.02.85 Bulletin 85/7

(84) Designated Contracting States:
CH DE FR GB LI

(71) Applicant: PITNEY BOWES, INC.
Walter H. Wheeler, Jr. Drive
Stamford Connecticut 06926(US)

(72) Inventor: Dlugos, Daniel F.
12 Twin Brook Drive
Huntington, Ct. 06484(US)

(74) Representative: Lehn, Werner, Dipl.-Ing. et al,
Hoffmann, Eitle & Partner Patentanwälte Arabellastrasse
4 (Sternhaus)
D-8000 München 81(DE)

(54) System for printing encrypted messages with bar-code representation.

(57) A system for the metering of encrypted postage and similar indicia includes a device (32) for printing such indicia and a device (34) for reading such indicia. The printing is accomplished with a bar-code printer driven by signals obtained from a keyboard (48) and from an encryption circuit. The reading is accomplished with a bar-code reader to retreive the characters, and permit the comparison of the separated coded data with a reference code to determine the accuracy of the printed material. Both the data and the code area imprinted by a bar-code indicia, a portion of the code being set aside for the data and a portion of the bar-code being set aside for encryption purposes. Thereby, the two portions can readily be separated to allow for automatic reading of the bar code for extraction of the message, while also allowing for automatic verification (54) by use of the encrypted material.

EP 0 132 782 A2

./...

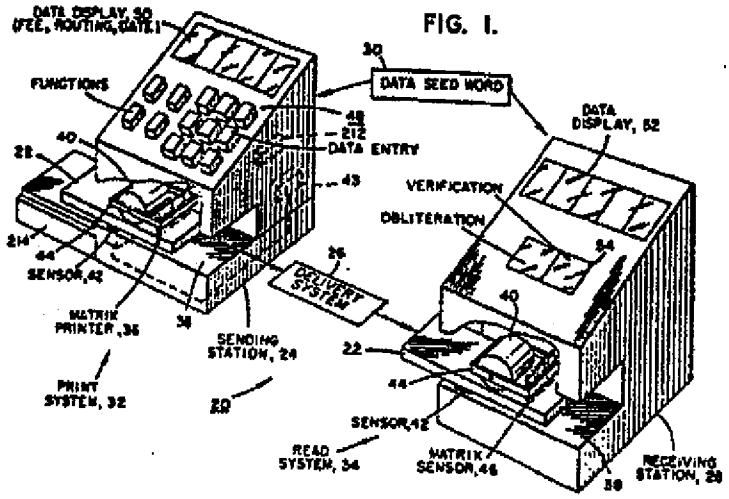

DATA DISPLAY, 50
(FEE, ROUTING, DATE.)
FUNCTIONS
48
212
DATA ENTRY
43
40
22
214
44
SENSOR, 42
MATRIX
PRINTER, 36
PRINT
SYSTEM, 32
38
SENDING
STATION, 24
20
30
DATA SEED WORD
DATA
DISPLAY, 52
VERIFICATION
OBLITERATION
54
26
DELIVERY
SYSTEM
40
22
44
SENSOR, 42
READ
SYSTEM, 34
MATRIX
SENSOR, 46
38
RECEIVING
STATION, 28

FIG. 1.

0132782

SYSTEM FOR PRINTING ENCRYPTED MESSAGES WITH BAR-CODE REPRESENTATION

This invention relates to devices for the metering of postage and similar indicia and, more particularly, to a metering device including electronic circuitry for the encryption of the indicia to be printed.

Reference is hereby made to copending related patent applications assigned to the same assignee as this application; application of John Clark entitled "System Having A Character Generator For Printing Encrypted Messages", serial No. 515 073, filed on July 19, 1983, application of John Clark and Daniel Dlugos entitled "System For Printing Encrypted Messages With A Character Generator And Bar-Code Representation", serial No. 515 072, filed on July 19, 1983; and application of John Clark, Alton Eckert and David Warren entitled "System For Printing And Reading Of Encrypted Messages", serial No. 515 760, filed on July 21, 1983.

Postage meters find extensive use, both in the United States and abroad, for imprinting postage on objects to be mailed. The postage may be applied by a self-sticking label which is imprinted by a print head enclosed within the meter, the label then being placed in adhering contact on the letter, parcel or other object to be mailed. Alternatively, the postage may be printed directly on the outer wrapping of the object being mailed. The printing apparatus is also capable of printing a short message in addition to the amounts of the postage so that, if desired, the meter can be used for the imprinting of suitable indicia designating instructions and/or routing for transport by private carrier as well as by the mail. Furthermore, if desired, the meter may be utilized for the imprinting of yet other forms of labels, such as tax stamps, assuming that governmental approval for such tax stamps is obtained.

A serious problem which has been encountered in the use of imprinted postage is the fraudulent adulteration of such postage labels whereby, in effect, the person adulterating the postage is stealing postage. A fraudulent label may enable someone to obtain postage, or in the case of a tax stamp, to avoid paying the tax.

to overcome
e or a
postage and
/or for print-
d/or for veri-
tures as

ircuitry for the
print head which
nprint both the
with the encryp-
the form of a bar
nicate data
communicate
two sets of
n be readily
extraction
sage and for
code. An
cuitry for
corporation
tering the
amount of
sender and

Thereby, the message imprinted on the
elated to the encryption markings. In the
t the message is altered, either the
markings cannot be decoded or, if decoded,
ing legend does not agree with the legend
on the label.

In Figure 1, a system 20 incorporates the invention for the transmission of a mailpiece or package 22 from a sending station 24 via a delivery system 26 to a receiving station 28. The term "package" is used only by way of example to illustrate the variety of objects which are sent from one location to another, both by use of the mail and by private carrier. Thus, the term "package" includes mailpieces such as letters, flats, envelopes, parcels and other objects which are sent via the mail, and have a surface for receipt of imprintings of postage and/or other indicia including messages. The term "package" also includes labels in those situations wherein the indicia or message is imprinted on a label which is then affixed to a mailpiece, in the case of postage, or to some other object such as bottle wherein the label is a tax stamp. The delivery system 26 may be any one of a number of systems such as, for example, a parcel delivery service or the postal service. The portrayal of the system 20 in Figure 1 is stylized to facilitate explanation of the invention, with portions of the stations 24 and 28 being cut away to show components thereof utilized in the imprinting and reading of data on the outer cover,

such as an envelope, of the mailpiece 22.

In accordance with the invention, the data is encrypted to ensure the validity of the data. The data includes, typically, the fee or postage, the date, a serial number of the sending station 24, and, if desired, a zip code or other form of routing code for automated sorting of the mailpieces 22. The encryption is accomplished by coding circuitry, to be described hereinafter, which utilizes a seed word in developing the code. The seed word is obtained from a base seed word 30 placed in both the sending station 24 and the receiving station 28, the base seed word 30 being altered in a manner to be described, in accordance with the date, the fee, and the serial number of the sending station 24 to provide the seed word utilized by the coding circuitry. The sending station 24 includes a print system 32 for imprinting the data on the mailpiece 22, while the receiving station 28 incorporates a corresponding read system 34 for reading the data imprinting on the mailpiece 22.

The print system 32 comprises a matrix printer 36 which includes a well known set of electronically actuated dot printing points in a printing head which, in accordance with electrical signals applied to respective ones of the points, imprints a row of dots

which represent a portion of a letter, numeral, or other character. For example, such a printing head may incorporate ink jets or, alternatively, may employ heat or light in the case wherein heat-sensitive labels or light-sensitive labels are utilized. The mailpiece 22 is moved along a platform 38 of the sending station 24 by a roller 40, the roller 40 advancing the mailpiece 22 beneath the matrix printer 36 as the printer 36 imprints a succession of dots on the cover of the mailpiece 22. A sensor 42 detects the presence of the package 22 for activating the roller 40. The sensor 42 may have the form of any of a number of well known package sensors, to incorporate, for example, an electric eye or a roller which makes electrical contact with the roller 40. Thereby, a breaking of the light beam, or a breaking of the electric current signals the presence of the package 22 for activation of the roller 40 to advance the package 22. The roller 40 and the matrix printer 36 are positioned by means of a frame 44 within the sending station 24.

The receiving station 28 also incorporates a roller 40 and a sensor 42 for advancing a package along a platform 38. A connector 43, shown in phantom inside the sending station 24, is coupled to the sensor 42 for counting output signals of the sensor 42 to provide a

count of the respective packages 22 sensed by the sensor 42. The read system 34 includes a matrix sensor 46, the sensor 46 comprising a set of well known photo-electric sensors which are arranged along a row and positioned by a frame 44 as described previously for the sending station 24. The positions of the photo-electric sensors of the matrix sensor 46 corresponds to the positions of the print points of the matrix printer 36 so that the presence and absence of markings of the printer 36 can be sensed by the matrix sensor 46.

The sending station 24 further comprises a keyboard 48 and an alphanumeric display 50. The keyboard 48 includes function keys which identify the nature of the data which is being entered by data entry keys of the keyboard 48. Thus, for example, individual ones of the function keys are employed to identify the date, the amount of the fee, and routing data. The data to be entered appears in the display 50 after which it is entered into the electronic circuitry of the sending station 24 by pushing an enter key of the keyboard 48. The receiving station 28 also incorporates displays, there being a data display 52 as well as a verification display 54 which indicates that the message imprinted on the package 22 has been verified or that it has been obliterated so as to prevent veri-

fication.

With reference also to Figure 2, there is shown a mode of encripting alphanumeric characters of the message imprinted on the mailpiece 22. This mode of encryption, which may be referred to as variable void coding is accomplished by offsetting the dots imprinted by respective printing points of the printer 36 so as to create voids at locations which would normally, in the absence of encryption, have imprinted dot. The field of dots in Figure 2 is defined by a matrix of seven rows by five columns. Such a matrix is a standard matrix in the printing industry and, accordingly, is most readily employed in a postage meter or similar device for the imprinting of postage and transportation data on a mailpiece. While the invention is useful for fields of both larger and smaller arrays of dots than that disclosed in Figure 2, in order to facilitate explanation of the invention, it is to be assumed in the ensuing description that the 7 x 5 matrix is to be employed. Individual ones of the dots in Figure 2 are identified by the legends 56 while two exemplary displaced dots 56A and 56B are disclosed in phantom. The phantom view indicates the postions which a dot 56 would occupy in the presence of encryption, the normal position, indicated by solid lines, being present in

the absence of encryption. In particular, it is noted that the displacement associated with the encryption provides a void equal to one-half the width of the dot 56. Thus, as may be seen in the cross-bar of the letter "A" depicted in Figure 2, the offsetting of the dot 56B enlarges the space between neighboring dots, to the left of the dot 56B, while decreasing the space, between neighboring dots, to the right of the dot 56B. Accordingly, the void or space between one pair of neighboring dots is increased while the void or space between another set of neighboring dots is decreased. In the encryption process, only a relatively few of the dots of an alphanumeric character are so displaced, the remaining dots maintaining their regular positions to permit identification of the character imprinted on the mailpiece 22.

In accordance with a feature of the invention, a reference character without the displaced dots of the encryption process is compared to a received character having the displaced dots associated with the encryption process. The differences between the characters is thus a statement of the code.

Figure 2 also shows a grid 58 superposed on the character "A" to explain the operation of the matrix sensor 46. The spacing between photoelectric ele-

ments of the matrix sensor 46 corresponds to the spacing between the rows of the grid 58, the horizontal lines being parallel to the arrow 60 which designates the direction of movement of the mailpiece 22. The spacing between the rows of the grid 58 is smaller than the spacing between centers of the elements of the matrix sensor 46 so as to permit the reading of the dots or other shaped markings of the character imprinted by the printer 36. Similarly, the rate of reading by the matrix sensor 46 is increased to provide a spacing between columns of the grid 58 which is smaller than the spacing between the dots of the printed character so that the matrix sensor 46 is able to respond to the variations in spacing between the dots resulting from the displacement associated with the encryption. By way of example, the spacings depicted between centers of the dots of the character in Figure 2 are four times the spacing of the cells of the grid 58. Correspondingly, the grid 58 provides the read system 34 with a resolution four times that of the print system 32, and thereby enables the read system 34 to function even with characters that may have become partially obliterated, as well as in the situation wherein the alignment of the package 22 on the platform 38 in the receiving station 28 does not correspond precisely to the

corresponding alignment in the sending station 24.

With reference now to Figure 3A, there is provided a more detailed description of the components of the print system 32 of Figure 1. The drum 40 is mechanically coupled via a line 62 to drive unit 64 which rotates the drum 40 for advancement of the mailpiece 22. The same form of drive unit 64 is also provided in the read system 34 of Figure 4A, as will be described subsequently, for rotation of the drum 40 therein. The drive unit 64 comprises the mailpiece sensor 42, a motor drive circuit 66, a stepping motor 68, a gear train 70 mechanically coupled via a dashed line 72 to the motor 68, a shaft-angle pulser 74 also mechanically coupled via the line 72 to the motor 68, and an address counter 76.

In operation, the motor 68 is energized by the drive circuit 66 for rotation of the drum 40 via the gear train 70. The drive circuit 66 is triggered into operation by the sensor 42, and continues to operate the motor 68 until the sensor 42 ceases to sense the presence of the mailpiece 22. Thereby, the drum 40 is made to rotate a sufficient amount to move the mailpiece 22 past the drum 40. The momentum of the mailpiece 22 then carries it through the sending station 24, as well as through the receiving station 28 as

will be described substantively with respect to Figure 4A. The gear train 70 reduces the rate of rotation of the drum 40 to a much slower value than the rate of rotation of the output shaft of the motor 68 on line 72. The shaft-angle pulser 74 comprises well known circuitry such as that of a tachometer or encoder for providing an output electrical pulse to the counter 76 for each increment in rotation of the output shaft of the motor 68. Since the pulser 74 is mechanically locked to the drum 40 by the gear train 70, a counting by the address counter 76 provides a count which corresponds precisely to the position of the mailpiece 22 on the platform 38 of the sending station 24. The leading edge of the electric output signals of the sensor 42 on line 78 resets the counter 76 back to zero upon the arrival of the next mailpiece 22 at the sensor 42. The output count of the counter 76 will be utilized, as described hereinafter, for addressing components of the print system 32 for operation of the matrix printer 36.

The print system 32 further comprises an address generator 80, a timing unit 82 an address generator 84, a RAM 86 (random access memory) for the storage of data entered from other components including the keyboard 48 and the counter 43, a coder 88 for providing the encripting code as will be more fully described

in Figure 5, a memory 90, a memory 92, and a set of void units 94 for driving respective ones of a set of print points 96 of the matrix printer 36. Each void unit 94 is utilized for incorporating digits of the encryption code which are stored in the memory 92 into the printing process for displacing dots of the character matrix in accordance with the variable-void feature of the invention. Each void unit 94 comprises a shift register 98, two AND gates 101-102, and an OR gate 103. In the AND gate 102, of the input terminals thereof is complimented, this terminal being coupled along with a corresponding terminal (not complimented) of the gate 101 to the code memory 92.

In operation, a person utilizing the sending station 24 enters data into the RAM 86 by use of the keys of the keyboard 48. As has been noted hereinabove, the keyboard 48 is also coupled to the display 50 for displaying the data which is to be entered into the RAM 86. During entry of the data, the signals of the keys of the keyboard 48 are also applied to the address generator 80 to activate the generator 80 to address the RAM 86 to designate the locations wherein the data of the keyboard 48 is to be stored within the RAM 86. The generator 80 is also utilized for addressing the RAM 86 during the outputting of data from the

RAM 86 to the coder 88 and to the memory 90, the action of the generator 80 initiated by signals of the timing unit 82 during the outputting of the storage data. The timing unit 82 also initiates activity of the address generator 84 to designate locations within the memory 90 for receiving data from the RAM 86. The coder 88 utilizes the data of the ram 86 in providing the digits which are stored in the code memory 92, and the memory 90 is utilized for applying the data of the RAM 86 via the void units 94 to the print points 96 of the matrix printer 36.

During the first stage of the operation of the sending station 24, the data such as the amount of postage, the routing as via zip code, the date and the package count of the counter 43 are entered into the RAM 86 for the subsequent imprinting of a message on the package 22. The message includes the date, the package count, the serial number of the sending station 24, the delivery fee or postage, and optionally zip code and/or city, state of the origination. In accordance with the invention, the message also includes, in encrypted form, a verification of the message showing that the message was indeed printed by the sending station 24, and not by an impostor.

Accordingly, the second stage in the opera-

tion is the transfer of data from the RAM 86 to the coder 88 for the generation of the encrypted verification, and to the memory 90 for operation of the matrix printer 36. The first two stages are initiated sequentially in response to the aforementioned signals of the timing unit 82 to the generators 80 and 84. During the second stage of the operation, the coder 88 generates the requisite code and applies the digits for control of the encryption process to the code memory 92 in a manner to be described subsequently with reference to Figure 5.

The third stage of the operation begins when the package sensor 42 has detected the presence of a mailpiece 22 or other object such as a letter which is to be mailed. As has been noted above, the sensor 42 resets the counter 76 and initiates operation of the motor drive circuit 66 with the resultant counting of the counter 76. The counter 76 counts out successive addresses of both the print memory 90 and the code memory 92 for transferring the data contained therein to the matrix printer 36. During the transfer of data from the RAM 86 to the memory 90, the data is arranged in accordance with the rows of dots of the matrix of each character which is to be imprinted on the mailpiece 22. Thus, in response to each designation of

character by the keyboard 48, the RAM 86 makes available to the memory 90 the succession of dots for each row of the characters matrix as has been explained with reference to Figure 2. Accordingly, upon transfer of the data from the RAM 86 to individual sections of the print memory 90, respective sections of the memory 90 store the requisite sequence of dots which are to be applied by the corresponding print points 96 to the mailpiece 22 during the printing operation.

In response to the addressing by the counter 76, the data is read out of the respective section of the memory 90 and of the respective sections of the memory 92 into the corresponding void units 94 for application to the corresponding printheads 96. With respect to the operation of the void units 94, each void unit 94 operates in the same manner. In each void unit 94, data from the memory 90 is applied to an input terminal of the shift register 98 through which it is clocked at a higher rate than the entry of data from the memory 90 into the register 98. For example, the rate of clocking in the register 98 may be at a rate four times greater than the rate of entry of the data from the memory 90 into the register 98. The clocking is accomplished in response to clock pulses applied at terminal C from a clock (not shown) within the timing

unit 82.

The foregoing factor of four in the clock rate corresponds to the factor of four (described in Figure 2) between a dot of the printed character and a cell of the grid 58. Thus, as a digital signal enters the shift register 98 from the memory 90, the digital signal then propagates rapidly through the shift register 98 through successive cells thereof. As these digital signals propagate through the shift register 98, the mailpiece 22 is advanced by rotation of the drum 40. Each increment in time associated with the propagation from cell to cell of the shift register 98 corresponds to an increment in postion of the package 22. Each cell of the register 98 is provided with an output tap or terminal whereby a signal can be extracted after a predetermined amount of delay from the time of transfer of the signal from the memory 90 to the shift register 98.

Each row of the code memory 92 is coupled to a corresponding one of the void units 94. More specifically, as has been described above, in each void unit 94, an output line of the code memory 92 is applied to an input terminal of each of the gates 101-102. In response to the outputting of a logic 0 signal from the code memory 92, the AND gate 102 is activated due to

the complementing of its input terminal coupled to the memory 92. With the activating of the AND gate 102, the digital signals of the shift register 98 are coupled via the AND gate 102 and the OR gate 103 to the print point 96. In response to the outputting of a logic 1 signal from the code memory 92, the AND gate 102 is deactivated and the AND gate 101 is activated to pass a digital signal from the shift register 98 via the OR gate 103 to the printhead 96. Since the AND gate 101 is coupled to a cell of the register 98 downstream from the connection of the AND gate 102 to a cell of the register 98, the activation of the gate 101 results in a delay of the operation of the print point 96. In view of the continuous motion of the package 92 by the rotation of the drum 40, the delay introduced by the gate 101 results in a displacement of the position of the dots, such as the previously described displacement of the dots 56A-B of Figure 2. In view of the ratio of four cells of the grid 58 corresponding to the spacing between centers of the dots 56 of Figure 2, the delay of one of the registers 98 (as depicted by the connections of the gates 101 and 102 to the register 98) provides for a displacement equal to one-half the width of a dot 56 as depicted in Figure 2. Accordingly, for each occurrence of a logic 1 from the code mem-

ory 92, there is presented a corresponding displacement in the position of a dot of the character in Figure 2. For ease of portraying such displacements, only two such displacements are shown in the Figure, this being the displacement of the dots 56A-B. With the displacement, there is created a void at the site where the dot 56 would have been located in the absence of the encripting command from the signals of the code memory 92. Thus, a void unit 94 has introduced a void into the printed character so as to encrypt the character with a code that is to be utilized for verifying the printed message.

With reference to Figure 4A, the read system 34 operates in a manner complementary to that of the print system 32 of Figure 3A. As has been noted hereinabove, the receiving station 28 includes a drum drive unit 64 for rotating a drum 40 to advance the package 22 beneath the matrix sensor 46. The reset line 78 of the drive unit 64 is also utilized to reset a timing unit 106 which provides timing signals at terminals T1 and T2 for operating components of the system 34 as will now be described.

The read system 34 comprises a RAM 108, a correlator 110, an address generator 112, a memory 114, buffer storage unit 117-118, a RAM 120, an address gen-

erator 122, a subtractor 124, a memory 126 and a correlator 128. Also included in the system 34 are the data display 52 and the verification display 54, previously described with reference to Figure 1, as well as an optional display 52A. In addition, the system 34 includes a coder 88 and a code memory 92 which have been described with reference to Figure 3A.

In operation, upon the sensing of a mailpiece 22 at the receiving station 28 (Figure 1), the address counter 76 of the drive unit 64 addresses the RAM 108 to enter data from the matrix sensor 46 as the mailpiece 22 moves along the platform 38. The counting of the counter 76 is synchronized with the movement of the package 22 by the shaft-angle pulser 74. The counter 76 includes an additional terminal designated as terminal A in Figures 3 and 4, for providing a high speed counting at a rate four times that of the addressing rate utilized in the print system 32 of Figure 3A. This is readily accomplished by deleting the least-significant bits from the lower rate counting output terminal of the counter 76. The counting rate at the terminal A of the counter 76 is utilized in Figure 4A to address the RAM 108 at the rate corresponding to the density of the cells of the grid 58 in Figure 2. Thus, as the package 22 advances past the matrix sensor

46, the signals of the photo-electric elements of the matrix sensor 46 are sampled and are entered into the RAM 108 at the rate four columns of the grid 58 for each column of dots 56 of the character in Figure 2. In addition, the close spacing of the photo-electric elements of the matrix sensor 46 provide for four rows of samples, in the grid 58 for each row of dots 56 of the character in Figure 2. The matrix sensor 46 extends well beyond the top and bottom of the text printed on the bottom of the mailpiece 22 to be able to receive the printed message even if the imprint on the mailpiece 22 is slightly offset from the position of the matrix sensor 46.

The operation continues with the correlator 110, the address generator 112, the memory 114 and the buffer storage units 117 and 118. The operation of the correlator 110 is initiated by a signal of the timing unit 106 subsequent to the storing of the data in the RAM 108. The timing signal is obtained with the aid of the package sensor 42 which changes the state of the signal on line 78 from a logic 1 to a logic 0 when the mailpiece 22 has completely passed by the sensor 42. Thereby, the timing unit 106 is signalled by the sensor 42 that the reading of data by the matrix sensor 46 has been completed and that accordingly, the stored data

can be outputted from the RAM 108.

The correlator 110 and the address generator 112 react with the RAM 108 in a well known fashion for transferring the message from the RAM 108 to the storage unit 117. Automated readers of printed matter are commercially available, and are equipped with circuitry for extraction of the message even if the object being read is slightly offset from the orientation of the reading head. Such an adjustment offsetting is readily accomplished by correlating received symbols with symbols stored in a reference memory, this being the memory 114. By cycling through the various storage cells of the RAM 108, the correlator 110 correlates the individual characters stored in the RAM 108 with the reference characters of the memory 114 so as to determine which characters, or symbols have actually been sensed by the matrix sensor 46. When a correlation is obtained between the received symbol and the reference symbol, the correlator 110 triggers the generator 112 to address a location in the storage unit 117 for entering the received symbol. Simultaneously, with the using of the storage unit 117, the generator 112 also addresses the storage unit 118 for entering the reference symbol from the memory 114. The character, or symbol, stored in the storage unit 117 differs from

that stored in the storage unit 118 in that the received character of the storage unit 117 includes the variable voids of the encryption process while the characters stored in the storage unit 118 is free of the voids of the encryption process. The succession of reference characters entered into the storage unit 118 are also applied via the memory 114 and the address generator 112 to the RAM 120 so as to store the data of the complete message in the RAM 120.

The final step in the operation of the read system 34 can now be accomplished by utilizing the data stored in the storage units 117-118 and in the RAM 120. First, it is noted that the reference symbols are provided by the memory 114 to the correlator 110 and to the storage unit 118 in the form of the dot matrix presented in Figure 2 so that a comparison can be made between the dot-matrix representation of the character in the storage unit 117. With respect to the RAM 120, the memory 114 provides only a digital word identifying each of the characters. Since the storage unit 118 contains the complete dot-matrix representation of each symbol, the symbols are readily outputted from the storage unit 118 directly to the data display 52. Thereby, as the characters are successively outputted from the storage units 118 to the display 52, the en-

tire message builds up within the display 52 for presentation to a person utilizing the receiving station 28 of Figure 1.

In accordance with a feature of the invention, the verification of the received message is obtained by comparing the received characters of the storage unit 117 with the corresponding reference characters of the storage units 118. This is accomplished by subtracting, cell by cell in accordance with the grid 58, the data stored in the storage unit 118 from the data stored in the storage unit 117. The cell-by-cell process is implemented by sequentially addressing the respective storage locations by the address generator 122. The address generator 122 is operated in response to a timing signal from the timing unit 106 so as to implement the foregoing addressing after the correlator 110 has directed the entry of the characters into the storage units 117-118. The subtraction is accomplished by the subtractor 124, and the results of the subtraction are entered into the memory 126 in response to an addressing thereof by the generator 122. It is readily appreciated that, with reference to a comparison of the characters stored in the two storage units 117-118, that in the event that corresponding cells of the grid 58 have equal value of logic signals,

the logic 0 or a logic 1, then the output of the subtractor 124 is zero. On the other hand, if a void is present due to the encryption process, then the logic value stored at the corresponding grid cells will differ and, accordingly, the subtractor 124 will output a logic 1 to the memory 126. Thereby, the memory 126 stores a representation of the encryption code as received by the receiving station 28. Assuming that there has been no obliteration of the printed message, and that the printed message is a valid message as distinguished from a message printed by an impostor, then the array of data stored in the code memory 126 will be identical to the array of data stored in the code memory 92 of Figure 3A.

The data stored in the code memory 126 is to be compared with the data of the code memory 92 to determine that a valid message has been transmitted. Accordingly, the coder 88 of Figure 4A is activated with the received data in the RAM 120 in the same manner as was described previously for the activation of the coder 88 with the data of the RAM 86 in Figure 3A. The coder 88 (Figure 4A) then generates the reference code for storage in the memory 92. The codes of the memories 126 and 92 are then correlated by the correlator 128 which signals the display 54 to indicate a

verification upon the obtaining of a good correlation, or to show obliteration, in the event that an inadequate correlation is obtained. It is to be understood that an inadequate correlation can be due to either obliteration or the act of an impostor. In either case, the user of the receiving station 28 has been alerted to the fact that the message imprinted on the mailpiece 22 cannot be verified. Both the correlators 128 and 110 are understood to include an adjustable reference level against which the correlation is performed since, in practice, it must be assumed that various markings such as dirt and scratches will appear on the package 22 which will provide a less than perfect correlation even with a valid message.

If desired, the display 52A may be used to present the alphanumeric indicia with the variable void coding. For this purpose, the output signals of the storage unit 117, in addition to being coupled to the subtractor 124, are also coupled to the display 52A. In addition, the foregoing output signals of the subtractor 124 are also coupled to the display 52A, these signals being synchronized with corresponding ones of the storage unit 117 and indicating the presence of a displaced pixel. In response to the subtractor signals, the display 52A provides for a blinking or

coloring of the displaced pixels so that personnel utilizing the read system 34 can readily observe the coding of the indicia.

With reference to Figure 5, there is shown a simplified representation of a coder 88. Coding devices are readily available commercially and by way of example, a maximal-length shift-register code generator is described in Figure 5. The coder 88 comprises a shift register 130, which stores a seed word, and is driven by a clock 132. A set of modulo-2 adders 134 sum the contents of successive ones of the cells of the shift register, with the resultant sum being inputted to the first cell of the register 130. The contents of the right-hand cell of the shift register 130 is designated as the output terminal of the coder 88.

In accordance with a feature of the invention, the seed word is generated by use of input data relating to one or more parameters such as the date, the fee, the serial number of the sending station 24, and the count of mailpieces and other packages provided by the counter 43. Accordingly, the coder 88 further comprises a register 136 for receipt of the input data, a ROM (read only memory) 138 and three adders 141-143. The ROM 138 stores a set of seed words which are addressed in accordance with the three least

significant bits of the data, there being accordingly eight base seed words stored in the ROM 138. The selected base seed word is then added modulo-2 with the fee at the adder 141 and again added modulo-2 with the serial number of the sending station 24 at the adder 142, and again added modulo-2 with the piece count of the counter 43. The serial number is being permanently stored in the register 136. The output digital word of the adder 143 is then loaded into the shift register 130 to serve as the seed word from which the code is generated by the coder 38.

It is to be understood that the foregoing contributions to the seed word are presented by way of example. Thus, if desired, the contribution of the serial number and/or the fee may be deleted. The use of the date and the piece count in the composition of the seed word is advantageous in providing a seed word which varies from mailpiece to mailpiece and from day to day, a clear benefit for improved security. In the event that a microprocessor (not shown) be incorporated in the sending station 24 and the receiving station 28, other forms of codes can be generated such as those of the National Bureau of Standards based on the multiplication of pairs of large numbers.

The foregoing print system and read system

has provided an effective way of introducing an encrypted code into a printed message which can readily verify the validity of the message. The use of the variable voids permits the message to be read either manually or by machine, while obtaining the encrypted identification. It is also noted that the foregoing systems also are applicable for any form of printed symbol, whether readable manually or only by machine. Thereby, if desired, the imprintings on the mailpiece 22 can be accomplished with a set of nonsense symbols which are recognizable only by use of the stored reference symbols in the read system. Thereby, a system for assuring payment of the fee imprinted for postage, taxes and other purposes has been disclosed.

It is furthermore noted that the message need not be imprinted only on a flat type of package but that, if desired, the message may be imprinted on a label or stamp which can later be affixed by labeling equipment to a container such as a bottle. Thereby, the system of the invention can also be utilized for the affixation of tax stamps to liquor bottles as well as to other objects requiring a tax. The reading process can then be accomplished automatically, and has been described hereinabove, by use of a conveyor (not shown) to move the bottle or other objects past the

matrix sensor for reading the legend imprinted on the tax stamp or other label. Thereby, fraudulent stamps or labels can be detected.

COMBINATION OF CODED SYMBOLS WITH DATA SYMBOLS

By way of alternative embodiments, it is noted that the security can be obtained by having a set of characters which designate the date, the fee, the piece count and the serial number of sending the station, with additional characters being supplied as a code. The characters of the code are based on the values the date, the fee and the serial number as has been disclosed in the previous embodiment. The code characters may be applied after piece count, or interleaved therewith. In either event, a predetermined timing arrangement is utilized as to determine which of the characters represent the data, and which of the characters represent the code.

Figure 3B shows a print system 200 which is an alternative embodiment of the print system 32 of Figure 3A. The system 200 provides for the printing of data characters plus code characters, and includes many of the components of the system 32. The system 200 comprises a ROM (read-only memory) 201, a print memory

202, an address generator 204, an OR circuit 206, and a timing unit 208 which provides for the arrangement of the characters as is portrayed in the graph 210. Also included in the system 200 are components which have been previously described, namely, the display 50, the keyboard 48, the address generator 80, the timing unit 82, the address generator 84, the RAM 86, the coder 88, the print memory 90, the drive unit 64, the code memory 92, the matrix printer 36, and the drum 40. Since the print system 200 provides both the data and the coding by means of alphanumerics, the matrix printer 36 may be replaced by some other form (not shown) of alphanumeric printer if desired.

The operation of the system 200 follows that of the system 32. Thus, the coder 88 provides a code word based on the date, the fee, the serial number, and the piece count which then produces the code in the memory 92. The output terminals of the memory 92 provide an address for selecting a code symbol or code character from the ROM 201. The print memory 90, under instruction from the address generator 84, stores the data which is to be printed on the mailpiece 22. Similarly, the print memory 202, under instruction from the address generator 204 stores the code characters which are to be imprinted on the mailpiece 22. The operation

of the generators 84 and 204 is controlled by timing signals from the timing unit 82. The arrangement of the contents of the memory 202 follows that of the memory 90 so that the contents of the memory 202 can be applied directly to the matrix printer 36. The data of the memory 90 and the code of the memory 202 are coupled alternately via the OR circuit 206 to the matrix printer 36. Timing signals for operation of the read out of the contents of the memories 90 and 202 is accomplished by signals of the timing unit 208, the timing unit 208 being driven by an output signal of the address counter 76 of the drive unit 64. Thereby, as the drum 40 advances the package 22 before the printer 36, the printer 36 imprints the package with both the data characters and the code characters as is portrayed in the graph 210.

One relatively simple form of code which may be imprinted on a mailpiece or other form of package 22 consists of a four-digit number representing the piece count of the counter 43 followed by a one digit code number. The coding operation (Figure 5) involves the modification of a base seed word by key board-entered data such as the fee and the date. Other data such as the serial number and the piece count are entered automatically into the RAM 86 for use by the coder 88.

As an example of still further data which may be utilized by the coder 88, in lieu of the foregoing or in addition thereto, are the total amount of prepaid postage stored in a system of registers 212 and the weight of a mailpiece or package 22 as provided by a scale 214. The register system 212 and the scale 214 are connected to the RAM 86, as shown in phantom in Figure 3B, and also appear in Figure 1. With reference to Figure 5, the register 136 of the coder 88 would be enlarged to include the weight and total prepaid postage, and additional adders (not shown) such as the adder 141 would be employed to combine the weight and postage with the base seed word.

Figure 4B presents the companion read system 220 for the print system 200. The system 220 is substantially less complex than the read system 34, the reduced complexity being obtained by a manual entry of the printed data on the mailpiece 22 into the system 220. Upon entry of the printed data into the system 220, the date, the fee, the piece count and the serial number are utilized, as previously described with reference to the read system 34, to produce the corresponding code. If the piece weight is utilized, the package is weighted and the weight is entered at the keyboard. If the prepaid postage is utilized for

assumed transmission by the postal service, such value is known at the post office (herein the receiving station 28) so as to be enterable by the keyboard. In the read system 220, the regenerated reference code appears on a display for visual comparison by an operator of the system.

The system 220 comprises the keyboard 48, the display 50, the RAM 86, the coder 88 and the code memory 92 which have been previously described with reference to Figures 3A and 3B. In addition, the system 220 includes the ROM 201, previously described in Figure 3B and a display 222. In operation, the person using the system 220 reads the message printed on the mailpiece 22, and enters the characters via the keyboard 48. The keyboard 48 activates the display 50 to show the characters entered, thus, providing the message comprising the date, the fee, piece count and the serial number of sending station. The keyboard 48 also activates the RAM 86 to provide the date, the fee the piece count and the serial number (and the weight and prepaid postage if this date is utilized) to the coder 88 which utilizes this data to produce the code in the memory 92. The code words in the memory 92 then address a ROM 201 to produce the code characters on the display 222. In the event that the data has been improperly entered

into the keyboard 48, a bogus address may be applied by the code memory 92 to the ROM 201 in which case a fault indicator will be illuminated on the display 222 to alert the operator of the system. Alternatively, if there has been a tampering with the message imprinted on the package, the display 222 may show a set of code characters, however, the set shown on the display 222 will differ from that actually imprinted on the package 22. Thereby, the operator of the system 220 has been alerted to a tampering of the printed message.

With respect to the read system 220, it is noted that should it be desirable to have automatic reading instead of the manual inputting, the read system 34 of Figure 4A is readily modified to provide the function of the system 220 of Figure 4B. Such modification is attained by replacing the correlator 110 (Figure 4A) with a timing unit, corresponding to the timing unit 208 of Figure 3B, for alternately switching the data and the code characters received from the photosensor 46 into the buffer storage units 118 and 117. The ROM 201 would be connected between code memory 92 and correlator 128, and the buffer storage unit 117 would be coupled directly to the correlator 128. Thus, the correlator 128 would directly correlate the set of code characters which was read from the package

22 with the set of code characters of the reference. Upon obtaining a proper correlation, the display 54 would indicate verification of the printed message.

BAR-CODE EMBODIMENT

The message printed on the mailpiece 22 by the succession of characters, as disclosed in Figure 3B, may alternatively be printed by means of a bar code as is now disclosed in the print system 400 of Figure 3C. The print system 400 has components previously described with reference to the print system 200 of Figure 3B, these components being the keyboard 48, the RAM 86, the coder 88, the code memory 92 and the ROM 201. The operation of the system 400 follows that of the system 200 and, accordingly, the characters commanded by the keyboard 48 are applied by the RAM 86 to the coder 88, and also to a buffer storage unit 402. The coder 88 utilizes the information of the date, the fee, and the serial number of the sending station to generate the coded words which are stored in the memory 92. If desired, the piece count may also be utilized. The output lines of the memory 92 address the ROM 201 to select suitable alphanumeric characters which can be printed by a bar code printer. The system 400 further comprises an OR circuit 404 and a bar code printer 406,

with the OR circuit 404 being connected to output terminals of both the ROM 201 and the storage unit 402 for alternately coupling the output signals to the printer 406. The alternate coupling is accomplished by timing signals provided by a timing unit such as the timing unit 208 which was utilized in the system 200 of Figure 3B. The printer 406 is understood to include the generator and other circuitry commonly found in bar code printers for converting the character command signal to a succession of lines of the bar code (not shown). The printer 406 then imprints the bar code on the mailpiece 22. The presentation of the printed message on the mailpiece 22 follows that disclosed in the graph 210 of Figure 3B.

The companion read system 420 for the print system 400 is disclosed in Figure 4C. The system 420 functions in a manner analagous to that of the read system 34 of Figure 4A, and contains some of the components of the system 34 as well as components of the print system 400 of Figure 3C. The system 420 comprises the drum 40, the drive unit 64, the timing unit 106, the coder 88, the code memory 92, the ROM 201 and the verification display 54 previously disclosed in Figures 4A and 3C. In addition, the system 420 comprises a bar code reader 422 of well-known configura-

tion, a ROM 424 for converting output digital signals of the reader 422 to the actual symbol represented by the reader 422, a ROM 426 for converting the output digital signal of the reader 422 to the input digital format utilized by the coder 88, and a correlator 428. Both the bar code printer 406 of Figure 3C and the reader 422 as well as the actual code are well known and are in common use. A portion of a bar code is portrayed, by way of example, on the mailpiece 22.

In operation, the drum 40 advances the mailpiece before the reader 422, enabling the reader 422 to read the code and apply the resultant characters of the reading to the ROMs 424 and 426. The drum 40 is driven by the drive unit 64 which, as has been disclosed previously with respect to Figure 4A, activates the timing unit 106 to provide timing signals synchronized to the movement of the drum 40 and the package 22. The output data of the ROM 426, comprising the date, the fee, and the serial number of the sending station, and/or other data is loaded into the coder 88. The coder 88 utilizes the foregoing data to provide code words which are stored in the memory 92 and are applied as addresses to the ROM 201 for providing alphanumeric symbols corresponding to the code words. The generation of the alphanumeric symbols by the ROM

201 in Figure 4C is the same as the symbols generated by the ROM 201 of the print system 400 in Figures 3C, assuming that the bar code was validly imprinted on the mailpiece 22. The contents of the ROM 424 and 201 may comprise the actual form of the respective symbols or, alternatively, may comprise a digital word identifying the alphanumeric symbol. In either case, the contents of the ROM 424 and the ROM 201 are clocked out by signals of the timing unit 106 into the correlator 428. The correlator 428 correlates the symbols of the respective ROMs 424 and 201 to determine that the code characters actually read by the reader 422 agree with those predicted by the operation of the coder 88 based on the date, the fee, and the serial number of the sending station. Upon obtaining a satisfactory correlation, the correlator 428 activates the display 54 to show verification of the printed message.

It is further noted that a mailpiece sorting system (not shown) may be coupled to the bar-code reader 422 for use in those situations wherein a zip code or other routing code has been imprinted on the package. Upon recognition of the routing code, the sorter then dispenses various packages in a series of such packages into various bins for automatic sorting of mail and similar packages. The output signal of the

correlator 428 may be utilized to activate the sorter so that no sorting takes place unless the message imprinted by the bar code on the package 22 has been declared valid. Thereby, an automatic sorting system can be used with a secure routing indicia imprinted on the packages.

COMBINATION OF ALPHANUMERIC AND BAR CODES INDICIA

The alphanumeric print system 200 of Figure 3B and the bar-code print system 400 of Figure 3C may be combined to form the print system 600 of Figure 3D. In comparing Figures 3C and 3B with 3D, it may be seen that each of these systems employ the keyboard 48, the RAM 86 the coder 88, the code memory 92 and the drum 40. Accordingly, the combined system 600 uses the foregoing components to activate both the matrix printer 36 and the bar-code printer 406. In the physical construction of the system 600, the two printers 36 and 406 may be positioned side-by-side so as to provide, simultaneously, both the alphanumeric and the bar-code indicia.

If desired, the bar-code printer 406 could employ the apparatus of the matrix print head of the printer 36, in which case each bar of the code would be

printed as an array of closely spaced dots. Furthermore, if the alphanumerics and the bar code are to be printed sequentially, rather than side-by-side, then a single print head could be used for both imprintings with the control circuitry being alternately switched from the alphanumerics to the bar code. This system is advantageous in that it permits the automatic sorting of mail, the automatic verification of the indicia, as well as the manual reading of the indicia so that personnel handling packages and mail can visually identify the imprinted legends if they so desire.

The companion read system 620 is shown in Figure 4D. The system 620 incorporates components of the system 34 of Figure 4A for reading printed alphanumeric characters and other symbols. Also included are both the bar-code reader 422 and the matrix sensor 46 for reading respectively the bar code and the alphanumeric characters. Also included are the drum 40, the drive unit 64 and the timing units 106 of both Figures 4A and 4C. Interpretation of the bar code is accomplished with the aid of the ROMs 424 and 426, the coder 88, the code memory 92 and the ROM 201 of Figure 4C. The character processing is implemented by use of the RAM 108, the correlator 110, the address generator 112, the symbol memory 114, the buffer storage 118 and the

RAM 120 of Figure 4A. Also included, by way of a second channel in the signal processing of the system 620 are the coder 88, the code memory 92, the symbol ROM 201 and the correlator 128. The RAM 120, the coder 88 and the memory 92 function as was disclosed with reference to Figure 4A. By use of the ROM 201, addressed by the memory 92, the character predicted by the coding operation is attained in a manner corresponding to that disclosed in Figure 4C. The predicted character from the ROM 201 and the actually received character from the buffer storage units 118 are correlated by the correlator 128. The output of the correlation is applied to the verification display 54' along with the output of the correlator 428. Thereby, correlation and verification can be obtained from the examination of the bar code or from examination of the alphanumeric code characters. The display 54 will respond to a positive correlation from either of the correlators 428 and 128. The display 52 displays the characters which have been received, this includes both the data characters and the characters of the code. In the system 620, while the complete array of characters is displayed for an operator of the system, the correlation is accomplished automatically without aid of the operator, as distinguished from the manually-aided read-

system 220 of Figure 4B.

INTERLEAVING OF CODE WITH INDICIA

With reference now to Figures 3E, 4E and 6, there is described an alternative form of the print and read systems utilizing an interleaving of the code with the indicia by speckling the indicia with portions of a code disposed as 1's and 0's across the field of the indicia. Such speckling is shown in Figure 6, while the corresponding print system 800 and the read system 850 are shown, respectively, in Figures 3E and 4E.

The print system 800 is a modification of the system 32 of Figure 3A and incorporates the keyboard 48, the address generator 80, the piece counter 43, the coder 88, the drive unit 64, and the drum 40 shown previously in Figure 4A. Instead of the 7 by 5 matrix format previously described, a larger field is employed to more easily implement the speckling procedure. For example, a 9 by 9 or larger matrix may be employed. Accordingly, the matrix printer of Figure 3A has been replaced by a larger-format printer 36A in Figure 3E. The system 800 further comprises RAM's 802 and 804, ROM's 806 and 808, and a set of switches 810 of which there is one switch for each row of the indicia matrix.

Each switch 810 comprises two AND gates 811 - 812, and an OR gate 813.

The speckling procedure, as demonstrated in Figure 6, interjects light areas into the dark coloration of the indicia, such as the exemplary numerals 2 and 3 of Figure 6, and interjects dark areas into the relatively light coloration of the background. The logic 1's represent points of impact of the print head while the logic 0's represent areas where no markings have been applied by the print head. In each symbol field, regions have been set aside for the speckling, the speckling in each of the regions being done on a random or pseudorandom basis.

In operation, the keyboard 48 and the counter 43 input data into the memory 802 in accordance with addresses provided by the generator 80. As has been described previously, the counter 43 counts mail pieces, packages, and other forms of parcels and labels which pass by the matrix printer 36A for the imprinting of postage or other message. A mailpiece 22 is shown in phantom as it is moved past the head of the matrix printer 36A by the drum 40. The data stored in the memory 802 forms the message which is to be imprinted on the mailpiece 22. Other sources of data such as the weight and serial number, described hereinabove, have

been deleted in Figure 3E to facilitate the description. The data stored in the memory 802 is applied to the coder 88 for the formation of the field of 1's and 0's, which field is stored in the memory 804. The arrangement of the stored field is similar to that shown in the memory 92 of Figure 3A, the stored field being larger in the memory 804 to accommodate the larger array of the indicia of Figure 6.

The matrix printer 36A comprises a set of print points 96, as does the printer 36 of Figure 3A, for printing a set of dots to form each symbol of the indicia. The rows and columns of the dots for each symbol are stored in the read-only memory 806, the dots of the respective rows being applied via corresponding ones of the switches 810 to the respective print points 96 of the printer 36A. The stored data in the RAM 802 is applied to the ROM 806 as an address to select the sequence of symbols for which the ROM 806 is to supply the dots to the printer 36A. Each of the switches 810, in addition to receiving the dots for a specific row of a symbol, also receives the dots from the RAM 804 for a specific row of the code. The speckling is accomplished by momentarily operating individual ones of the switches 810 to substitute dots of the code for dots of the field of a symbol.

The selection of the speckled regions differs with the various alphanumeric symbols, the locations and sizes of the speckled regions being chosen so as to retain legibility of the symbols as demonstrated in Figure 6. The ROM 808 stores the location of each pixel in each of the speckled regions for each symbol, and is addressed by the RAM 802 concurrently with the addressing of the ROM 806. Thereby, the speckle data and the symbol data for the imprinting of the complete message are available in the memories 808 and 806.

In each switch 810, the AND gates 811-812 are connected to an output line of the memory 808, the connection to the gate 812 being complemented to provide for alternate actuation of the gates 811-812 by output signals of the memory 808. The gate 811 connects with the code memory 804, and the gate 812 connects with the symbol memory 806. The output terminals of the gates 811-812 are coupled via the OR gate 813 to the printer 36A. Thereby, in response to a logic 0 outputted from the speckle memory 808, dots of the symbol are printed, and in response to a logic 1 outputted from the speckle memory 808, dots of the code field are printed by the printer 36A. The drive unit 64 activates the three memories 804, 806 and 808 to output their respective signals concurrently with the operation of the drum 40,

such operation of the drive unit 64 conforming to the description presented above for the system of Figure 3A. Thereby, the print system 800 of Figure 3E interleaves speckles of the code field with the printed indicia in a manner which preserves legibility of the message while permitting personnel utilizing the system 800 to observe the nature of the coding.

The operation of the read system 850 of Figure 4E parallels that of the read system 34 of Figure 4A in that the received signals are first correlated against a reference to identify the received signals, after which identification specific portions of the indicia carrying elements of the code are compared against a regenerated replica of the code. The system 850 includes the drum 40, the drive unit 64, the timing unit 106, the coder 88, and the displays 52 and 54 which were previously described with reference to Figure 4A. Also included is a matrix photo sensor 46A for viewing the received indicia, the sensor 46A operating in a manner similar to that of the sensor 46 of Figure 4A but having additional photo sensing elements for the enlarged dot-matrix format of the indicia printed by the system 800 on an object such as the package 22.

The read system 850 further comprises address generators 852 and 854, RAM's 855, 856 and 857,

correlators 861-862, a memory 864, and gates 867-868. The arrangement of dots sensed by the sensor 46A is stored in the RAM 802 concurrently with an addressing of the RAM 802 by the drive unit 64 in synchronism with the operation of the drum 40 for positioning the package or mailpiece 22. A reference dot-matrix array for each symbol is stored in the memory 864 to be correlated against the message symbols of the RAM 802 by the correlator 861. The correlation is based on the complete symbol field (Figure 6) minus the portions reserved for the speckled regions. Thereby, the symbols of the message can be accurately identified by the correlation process.

In operation, upon attainment of a correlation, the correlator strobes the address generator 854 to address the memories 857, 855 and 856 to store, respectively, the dot-matrix pattern of the received symbols from the RAM 802, the identify of the received symbol, and the pixel locations of the corresponding speckled regions. The latter is stored in the memory 864 along with the dot-matrix patterns of the reference symbols. The symbols stored in the RAM 855 are outputted to the display 52 so that personnel can read the message.

Verification of the coded portions of the

message, so as to insure the integrity of the message, is accomplished as follows. The coder 88 is also coupled to the output terminal of the RAM 855 and, upon receipt of data in the message, regenerates the code and stores the code field in the RAM 804. The code and symbol data stored in the RAM 857, and the code data stored in the RAM 804 are then read out via the gates 867-868, respectively, to the correlator 862. This reading out is accomplished under control of the address generator 852 which operates in response to timing signals of the timing unit 106. The operation of the timing unit 106 has been described hereinabove. Thus, the generator 852 addresses the RAM's 857 and 804 after the storage of their respective data has been completed.

The generator 852 also addresses the RAM 856 to activate the gates 867-868 to pass the respective output signals of the RAM's 857 and 804. Such activation occurs only within the designated regions for the speckling of the code, such data being stored in the RAM 856. Thereby, the correlator 862 is able to correlate the regions of the code field presented in the speckling with the corresponding reference regions of the code field to verify that the received message is true. The correlator 862 then strobes the display 54 to indicate the verification.

Claims

1. A device (32, 200, 400, 600, 800) for the metering of encrypted messages, such as postage and similar indicia characterized by:

(a) an entry means (48) for the entry of data;

(b) means (86, 90) coupled to said entry means (48) for the storage of said data;

(c) an encryption circuit (88, 92) for developing a code word;

(d) means (36, 406) coupled to said storage means (86, 90) and to said encryption circuit (88, 92) for imprinting a bar-code representation of the data of said storage means and a code word (210) of said encryption circuit;

(e) means (82, 94; 201, 208) synchronized with said imprinting and coupled between said storage means (86, 90) and said encryption circuit (88, 92) for alter-

nately feeding data of said storage means (86, 90) and a code word of said encryption circuit (88, 92) to said imprinting means (36, 402).

2. A device according to claim 1, 2 or 3, characterized in that said imprinting includes a printhead (96) for imprinting marks on a printing medium (22).

3. A device according to at least one of the preceding claims, characterized in that said entry means comprises a keyboard (48) and in that said keyboard (48) includes means (40, 64, 66) for moving the printing medium (22) passed said printhead (36).

4. A device according to at least one of the preceding claims, characterized in that said printing medium is a package (22), said device further comprising timing means (42, 43) coupled to said moving means (66) for synchronizing said alternate feeding with the position of said package (22).

5. A system (20) for the printing (32, 200, 400, 600, 800) of encrypted messages wherein the messages are printed in a bar-code format on a printing medium (22) characterized by:

(a) a keyboard (48) for the entry of data;

(b) means (86, 90) coupled to said keyboard (48) for storing the data;

(c) encryption means (88, 92; 202) responsive to the data for producing a code (210) derived from the data;

(d) a bar-code printer (406) for printing a bar-code indicia on said medium;

(e) means (82, 94; 201, 202, 208) coupled to said storage means (86, 90) for alternately driving said printer (406) with data from said keyboard (48) and with elements of the code of said encryption means (88, 92, 202).

6. A system (34, 420, 620, 850) for reading of encrypted messages according to claim 7, characterized by:

(a) means (422) for reading said bar-code indicia on said medium;

(b) means (426, 88, 92, 201) coupled to said reading means (422) for regenerating said codes;

(c) means (428) for comparing a code read by said reading means (422) with a code of said regenerating means (426, 88, 92, 201) for verification (54) of said bar-code indicia.

7. A system according to claim 5 or 6, characterized in that said printer includes a printhead (96) and means (40, 64) for moving said medium passed said printhead.

8. A system according to at least one of the preceding claims 5 to 7, characterized in that said moving means (40, 64) includes means (42) responsive to positions of said medium (22) for synchronizing (43) said printer driving means (64) with the movement of said medium.

9. A system according to one of the preceding claims 5 to 8, characterized in that said reading means (34) includes a reading head for sensing indicia on said medium, means for translating said medium (22)

passed said reading head, and means (42) responsive to the position of said medium (22) for timing (106) said alternate driving means (64).

10. A device for verifying the presence of encrypted material presented serially with data in a bar-code format printed on a printing medium wherein the encrypted material is derived from the data characterized by:

(a) means (422) for reading bar-code indicia on said printing medium (22);

(b) means (426, 88, 92, 201) responsive to data read by said reading means (422) for generating the encrypted material; and

(c) means (428, 54) for preparing the regenerated encryption material with a reading of such material by said reading means to verify the indicia.

11. A device according to claim 10, characterized by means (106, 64) synchronized with a reading by said reading means for moving the printed medium (22) and a reading head of said reading means.

FIG. 1.

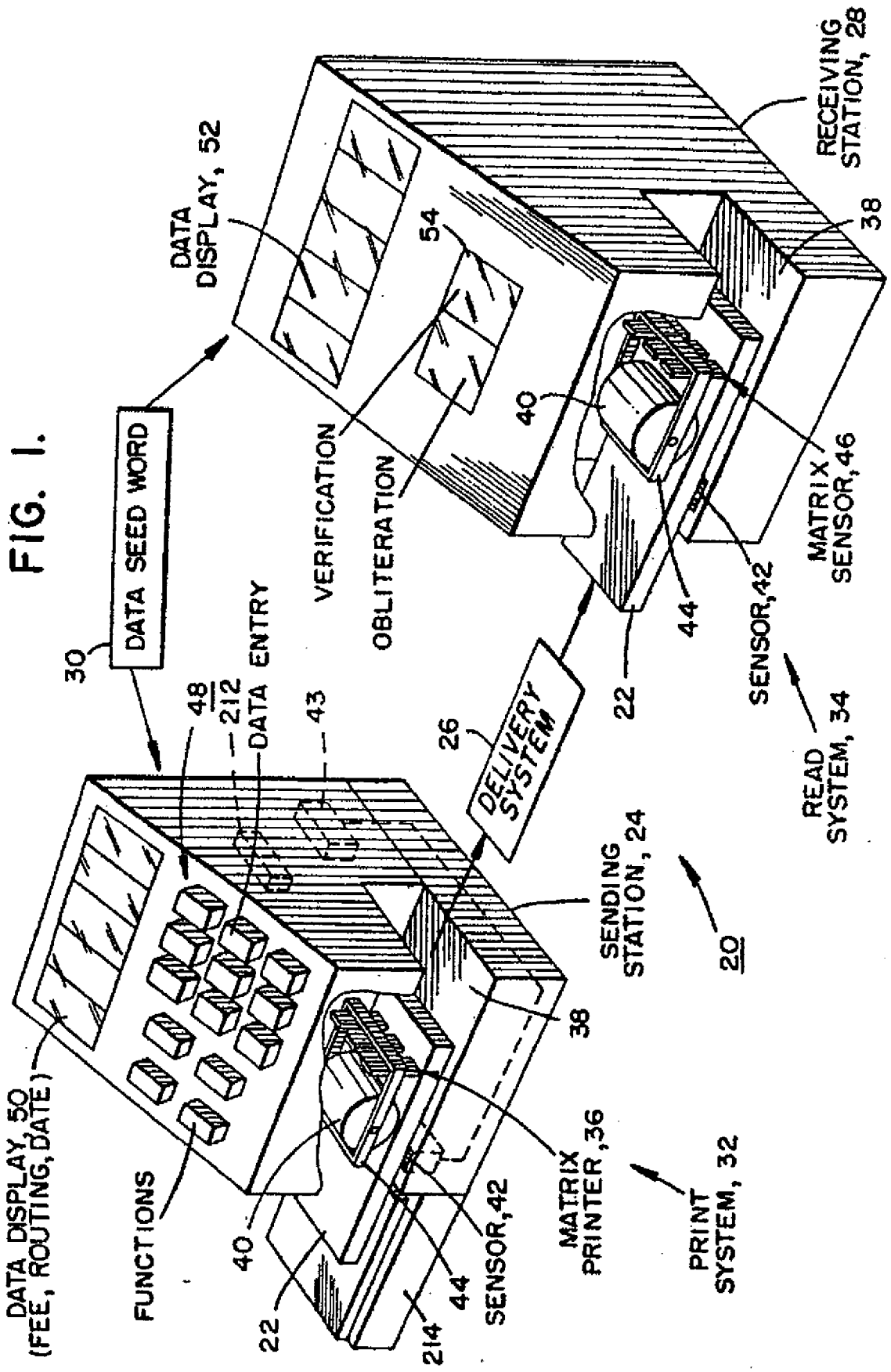

DATA DISPLAY, 52
RECEIVING STATION, 28
38
54
40
MATRIX SENSOR, 46
VERIFICATION
OBLITERATION
DATA SEED WORD
30
48
212
DATA ENTRY
43
26
DELIVERY SYSTEM
22
44
SENSOR, 42
READ SYSTEM, 34
SENDING STATION, 24
20
DATA DISPLAY, 50
(FEE, ROUTING, DATE)
FUNCTIONS
40
22
214
44
SENSOR, 42
MATRIX PRINTER, 36
38
PRINT SYSTEM, 32

FIG. 5.

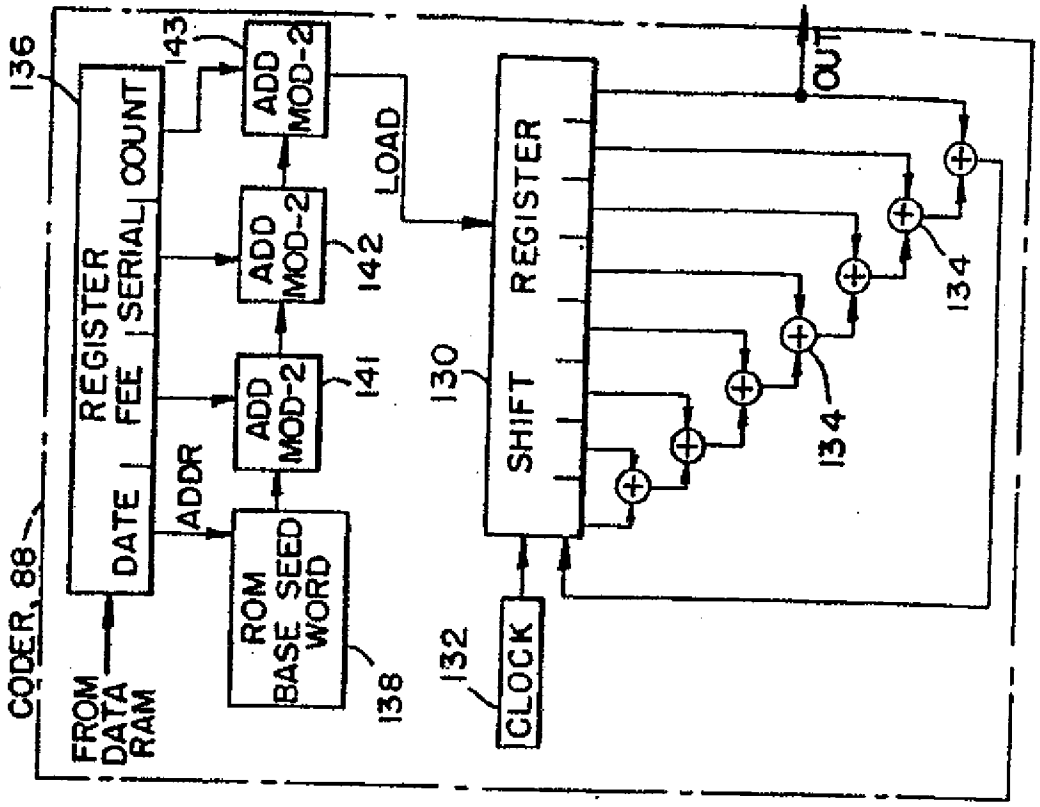

CODER, 88
FROM DATA RAM
REGISTER
DATE
FEE
SERIAL COUNT
ADDR
ROM BASE SEED WORD
138
ADD MOD-2
141
ADD MOD-2
142
ADD MOD-2
143
LOAD
SHIFT REGISTER
130
CLOCK
132
OUT
134
134
136

FIG. 2.

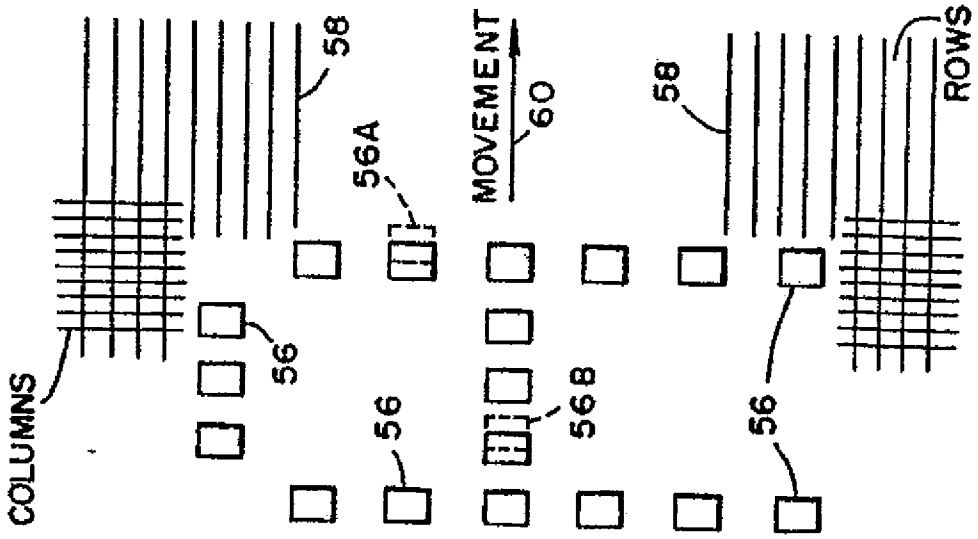

COLUMNS
56
58
56A
56
MOVEMENT
60
56B
58
56
ROWS

FIG. 3A.

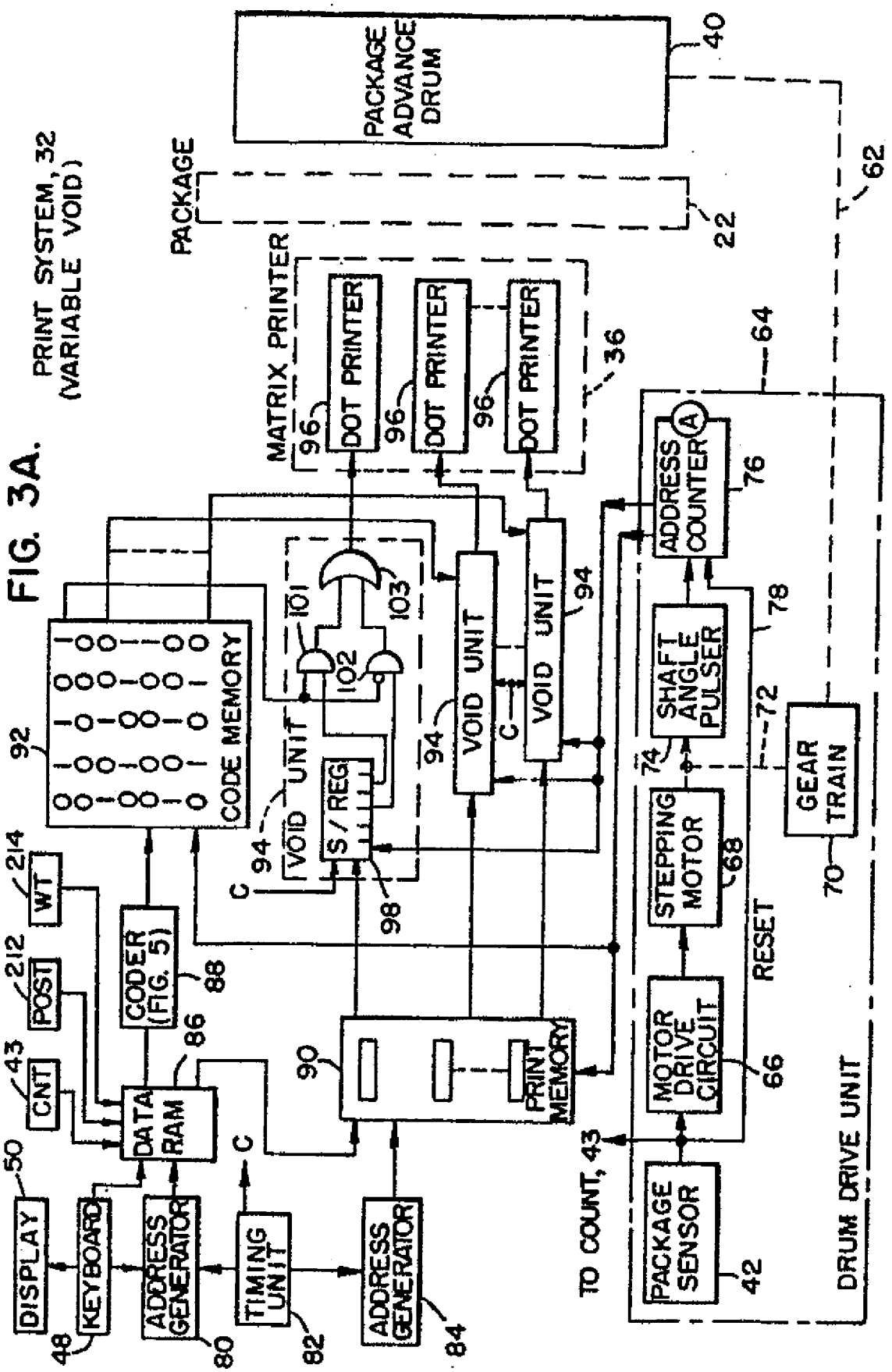

PRINT SYSTEM, 32
(VARIABLE VOID)
PACKAGE ADVANCE DRUM
40
PACKAGE
22
62
MATRIX PRINTER
DOT PRINTER
96
36
64
ADDRESS COUNTER
76
SHAFT ANGLE PULSER
74
78
72
GEAR TRAIN
70
STEPPING MOTOR
68
MOTOR DRIVE CIRCUIT
66
RESET
VOID UNIT
94
101
102
103
S/REG
98
CODE MEMORY
92
WT
214
POST
212
CODER (FIG. 5)
88
CNT
43
DATA RAM
86
PRINT MEMORY
90
DISPLAY
50
KEYBOARD
48
ADDRESS GENERATOR
80
TIMING UNIT
82
ADDRESS GENERATOR
84
TO COUNT, 43
PACKAGE SENSOR
42
DRUM DRIVE UNIT

FIG. 3B.

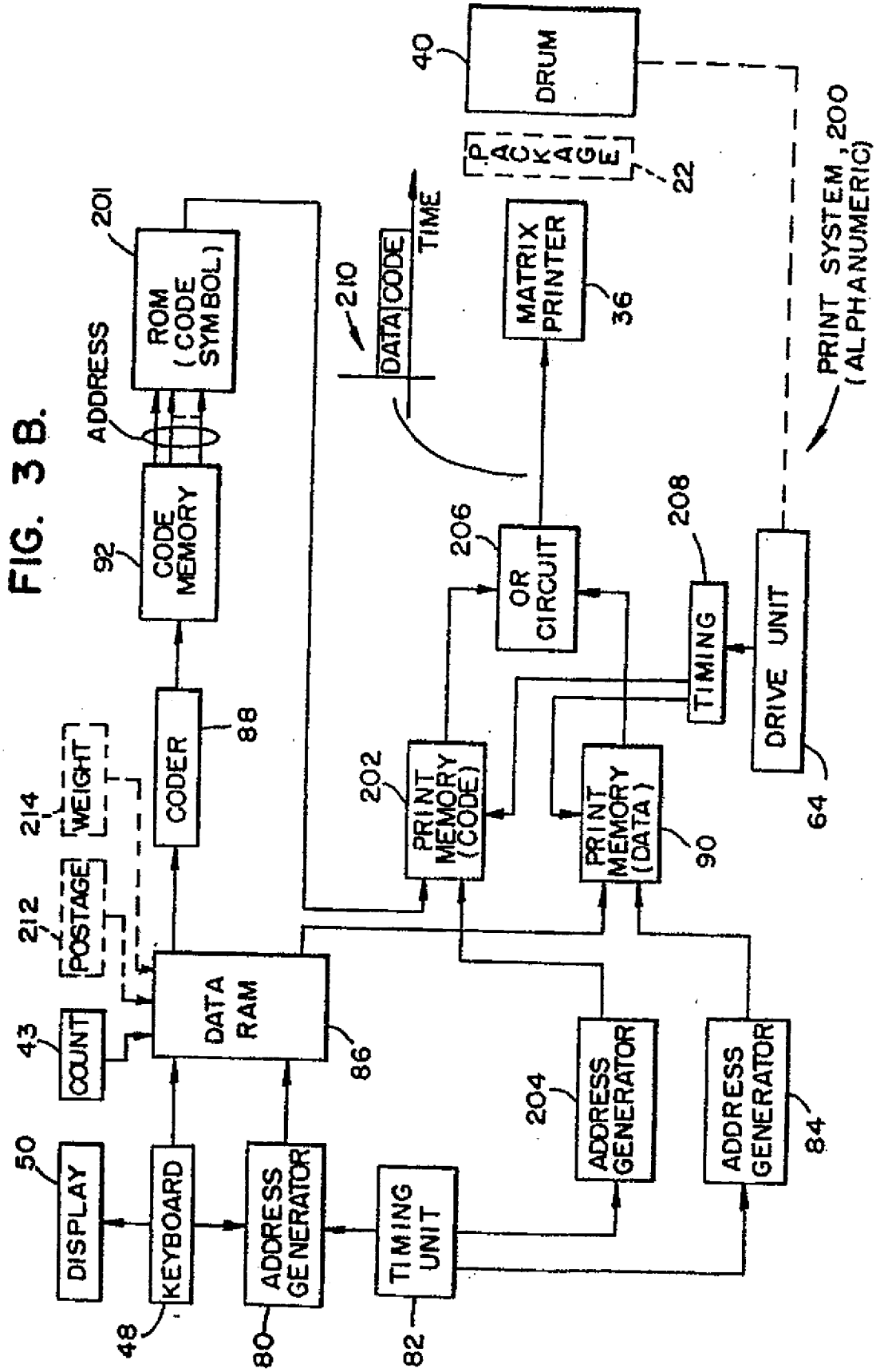

DISPLAY
50
KEYBOARD
48
ADDRESS GENERATOR
80
TIMING UNIT
82
COUNT
43
POSTAGE
212
WEIGHT
214
DATA RAM
86
CODER
88
CODE MEMORY
92
ADDRESS
ROM (CODE SYMBOL)
201
DATA
CODE
TIME
210
PRINT MEMORY (CODE)
202
PRINT MEMORY (DATA)
90
OR CIRCUIT
206
ADDRESS GENERATOR
204
ADDRESS GENERATOR
84
TIMING
208
DRIVE UNIT
64
MATRIX PRINTER
36
PLATEN
22
DRUM
40
PRINT SYSTEM, 200 (ALPHANUMERIC)

FIG. 3C.

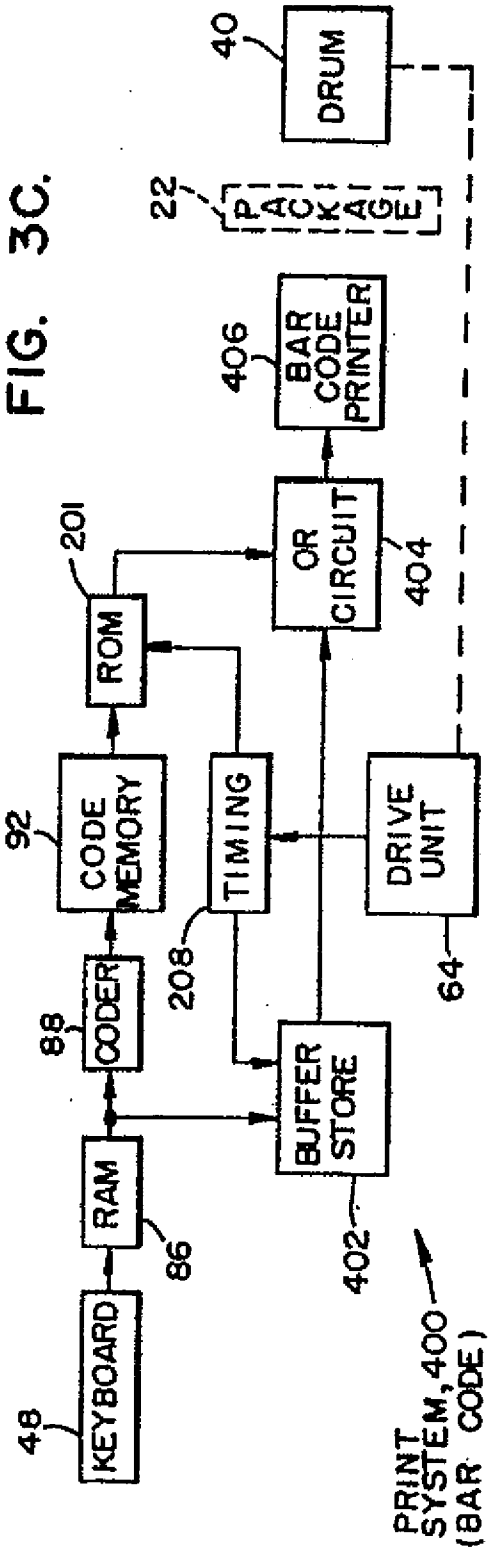

40
DRUM
22
PACKAGE
406
BAR CODE PRINTER
OR CIRCUIT
404
201
ROM
92
CODE MEMORY
TIMING
208
DRIVE UNIT
64
88
CODER
BUFFER STORE
402
RAM
86
48
KEYBOARD
PRINT SYSTEM, 400 (BAR CODE)

FIG. 4B.

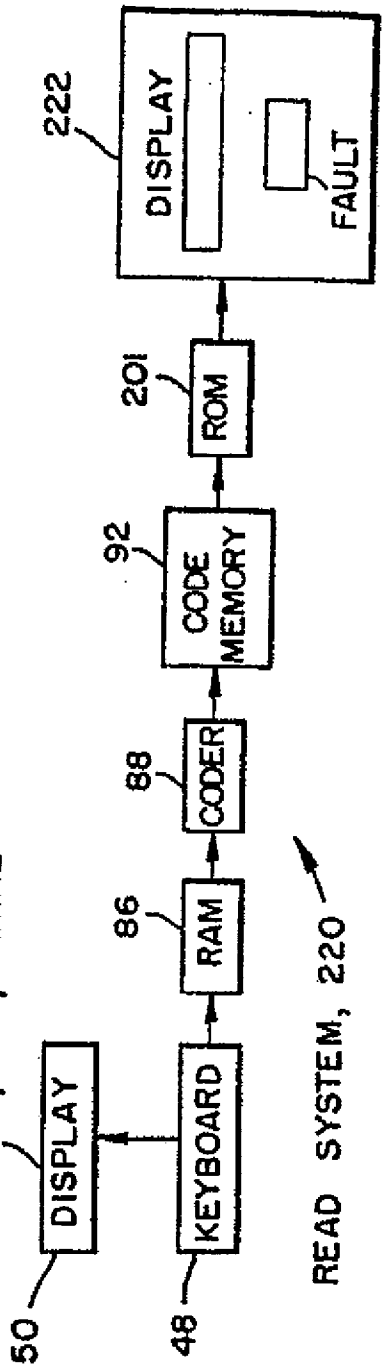
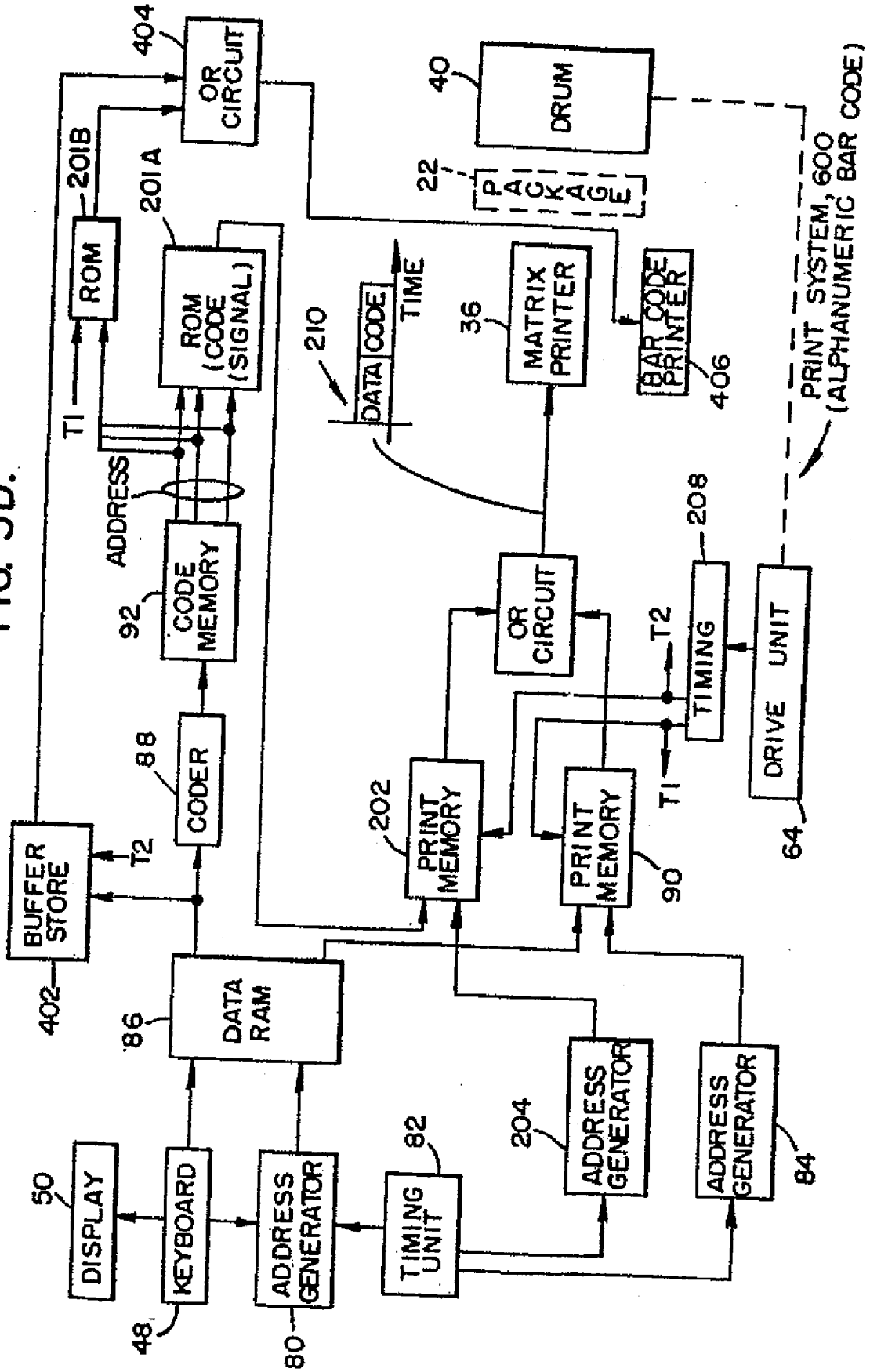

222
DISPLAY
FAULT
201
ROM
92
CODE MEMORY
88
CODER
86
RAM
DATE, FEE, SERIAL
DISPLAY
50
KEYBOARD
48
READ SYSTEM, 220

FIG. 3D.


404
OR CIRCUIT
201B
ROM
201A
ROM (CODE SIGNAL)
T1
ADDRESS
92
CODE MEMORY
88
CODER
BUFFER STORE
402
T2
86
DATA RAM
50
DISPLAY
48
KEYBOARD
80
ADDRESS GENERATOR
82
TIMING UNIT
204
ADDRESS GENERATOR
84
40
DRUM
22
PLACAGE
210
DATA CODE TIME
36
MATRIX PRINTER
406
BAR CODE PRINTER
PRINT SYSTEM, 600 (ALPHANUMERIC BAR CODE)
OR CIRCUIT
202
PRINT MEMORY
90
PRINT MEMORY
T2
T1
208
TIMING
DRIVE UNIT
64

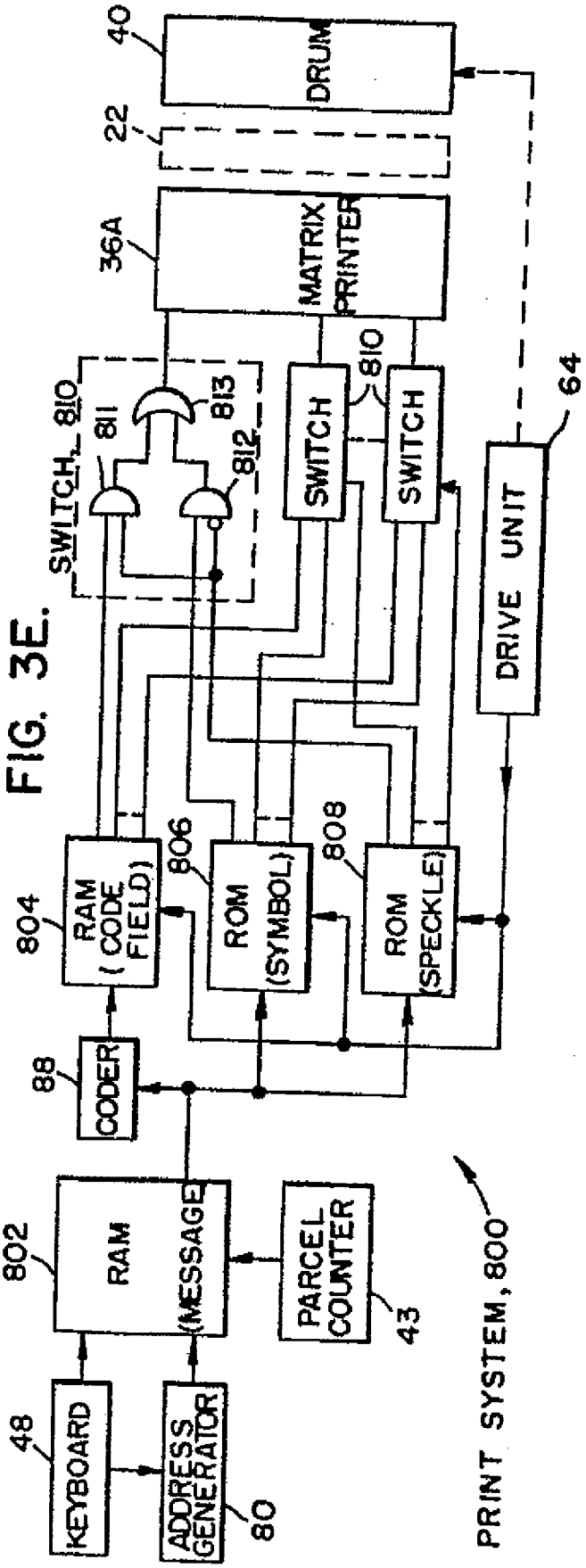

40
DRUM
22
36A
MATRIX PRINTER
SWITCH 810
81
813
812
SWITCH
810
SWITCH
64
DRIVE UNIT
804
RAM (CODE FIELD)
806
ROM (SYMBOL)
808
ROM (SPECKLE)
88
CODER
802
RAM (MESSAGE)
PARCEL COUNTER
43
48
KEYBOARD
ADDRESS GENERATOR
80
PRINT SYSTEM, 800

FIG. 3E.

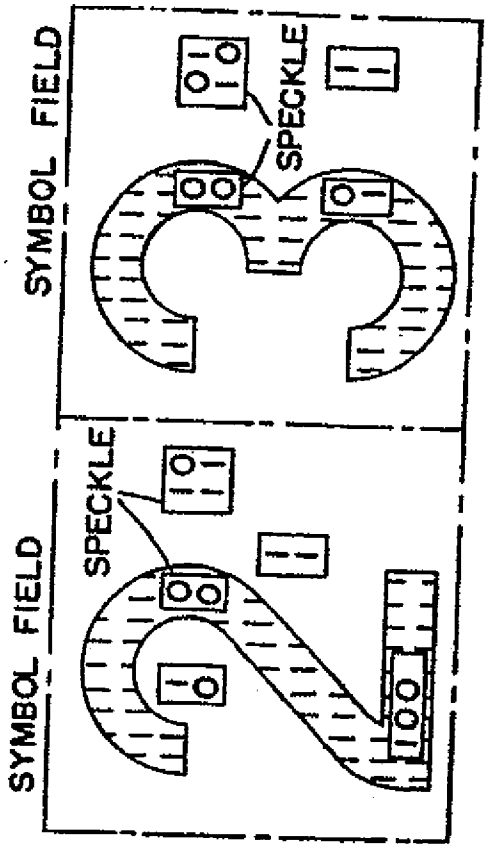

SYMBOL FIELD
SPECKLE
SYMBOL FIELD
SPECKLE

FIG. 6.

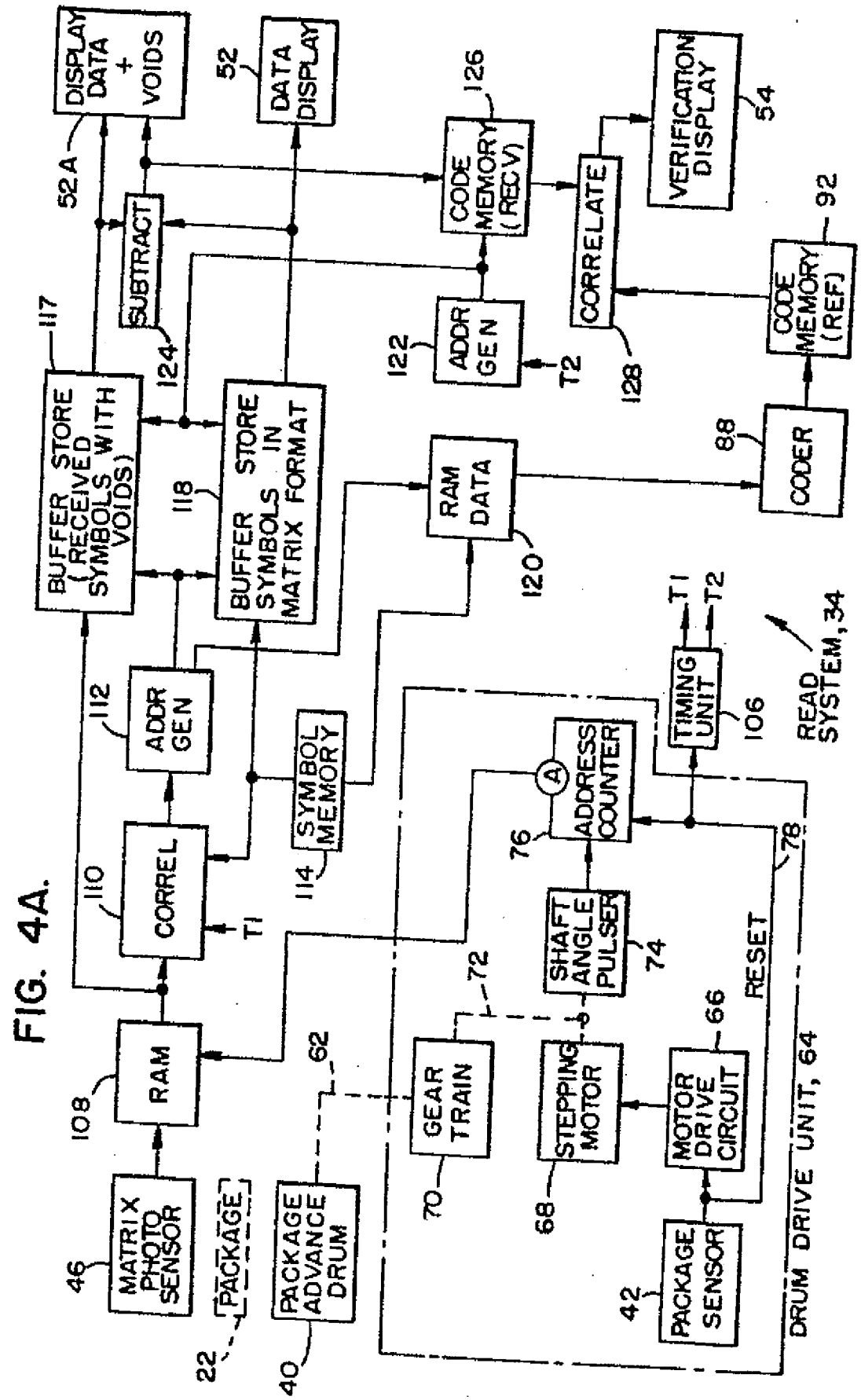
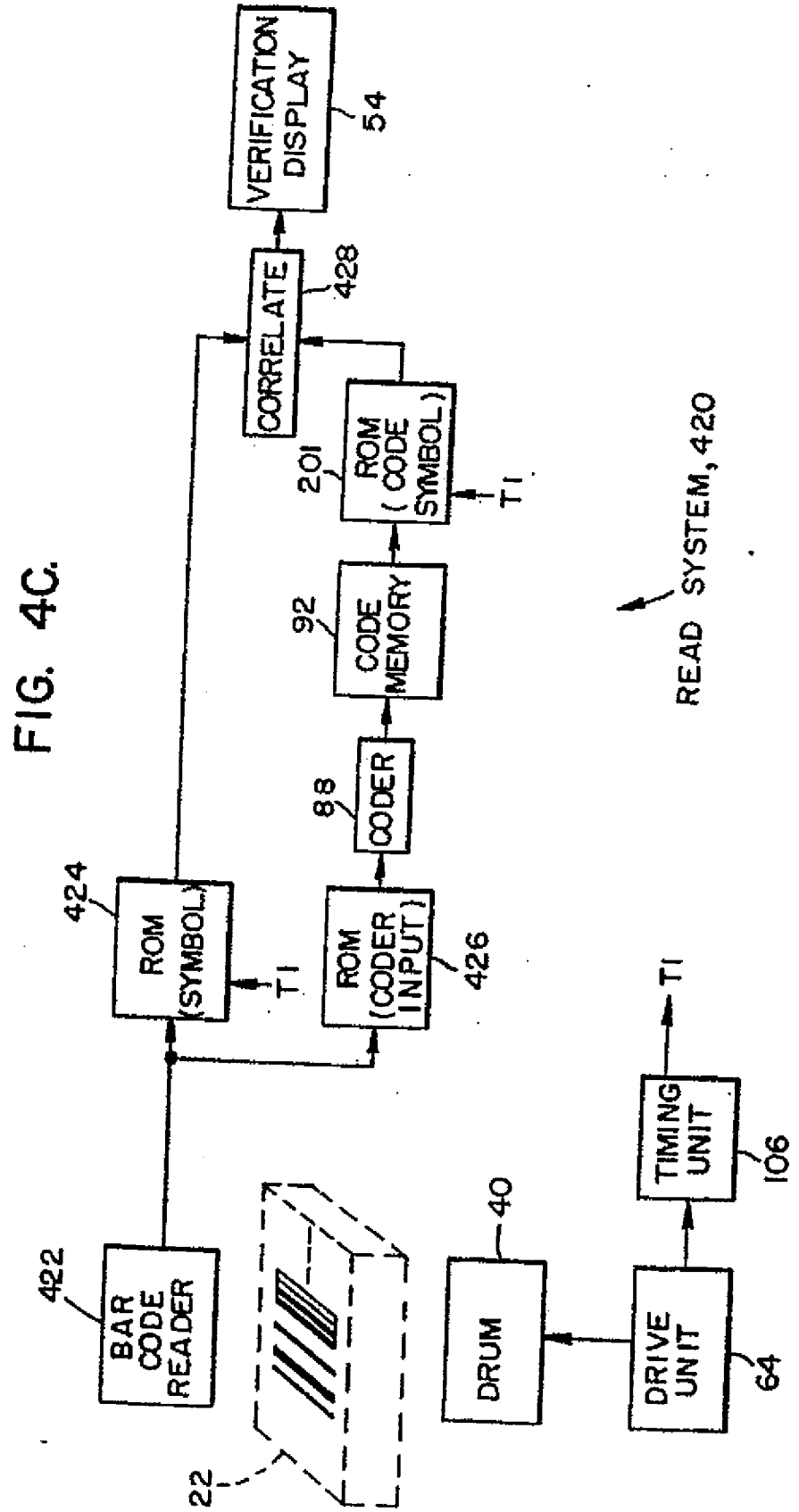

DISPLAY DATA + VOIDS
52A
DATA DISPLAY
52
CODE MEMORY (RECV)
126
VERIFICATION DISPLAY
54
SUBTRACT
117
124
ADDR GEN
122
T2
CORRELATE
128
CODE MEMORY (REF)
92
BUFFER STORE (RECEIVED SYMBOLS WITH VOIDS)
BUFFER STORE SYMBOLS IN MATRIX FORMAT
118
RAM DATA
120
CODER
88
ADDR GEN
112
SYMBOL MEMORY
114
TIMING UNIT
106
T1
T2
READ SYSTEM, 34
CORREL
110
T1
ADDRESS COUNTER
76
A
SHAFT ANGLE PULSER
74
72
RAM
108
62
GEAR TRAIN
70
STEPPING MOTOR
68
MOTOR DRIVE CIRCUIT
66
RESET
78
MATRIX PHOTO SENSOR
46
PACKAGE
22
PACKAGE ADVANCE DRUM
40
PACKAGE SENSOR
42
DRUM DRIVE UNIT, 64

FIG. 4A.

FIG. 4C.


READ SYSTEM, 420
VERIFICATION DISPLAY
54
CORRELATE
428
ROM (CODE SYMBOL)
201
T1
CODE MEMORY
92
CODER
88
ROM (CODER INPUT)
426
ROM (SYMBOL)
424
T1
BAR CODE READER
422
22
DRUM
40
DRIVE UNIT
64
TIMING UNIT
106
T1

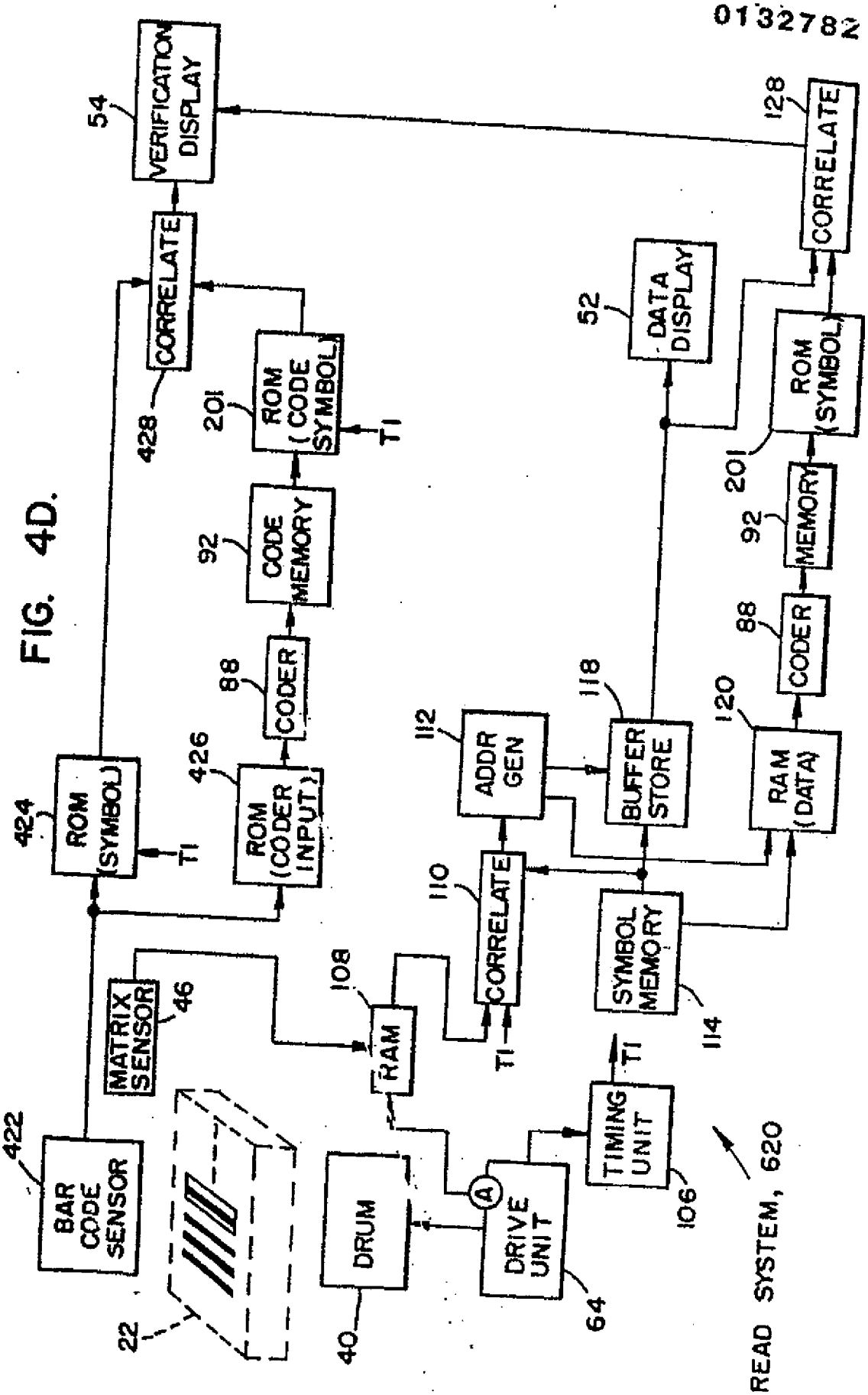

54
VERIFICATION DISPLAY
128
CORRELATE
52
DATA DISPLAY
428
CORRELATE
201
ROM (CODE SYMBOL)
T1
201
ROM (SYMBOL)
92
CODE MEMORY
92
MEMORY
88
CODER
88
CODER
424
ROM (SYMBOL)
T1
426
ROM (CODER INPUT)
112
ADDR GEN
118
BUFFER STORE
120
RAM (DATA)
110
CORRELATE
T1
108
RAM
MATRIX SENSOR
46
SYMBOL MEMORY
114
422
BAR CODE SENSOR
22
DRUM
40
DRIVE UNIT
64
TIMING UNIT
T1
106
READ SYSTEM, 620

FIG. 4D.

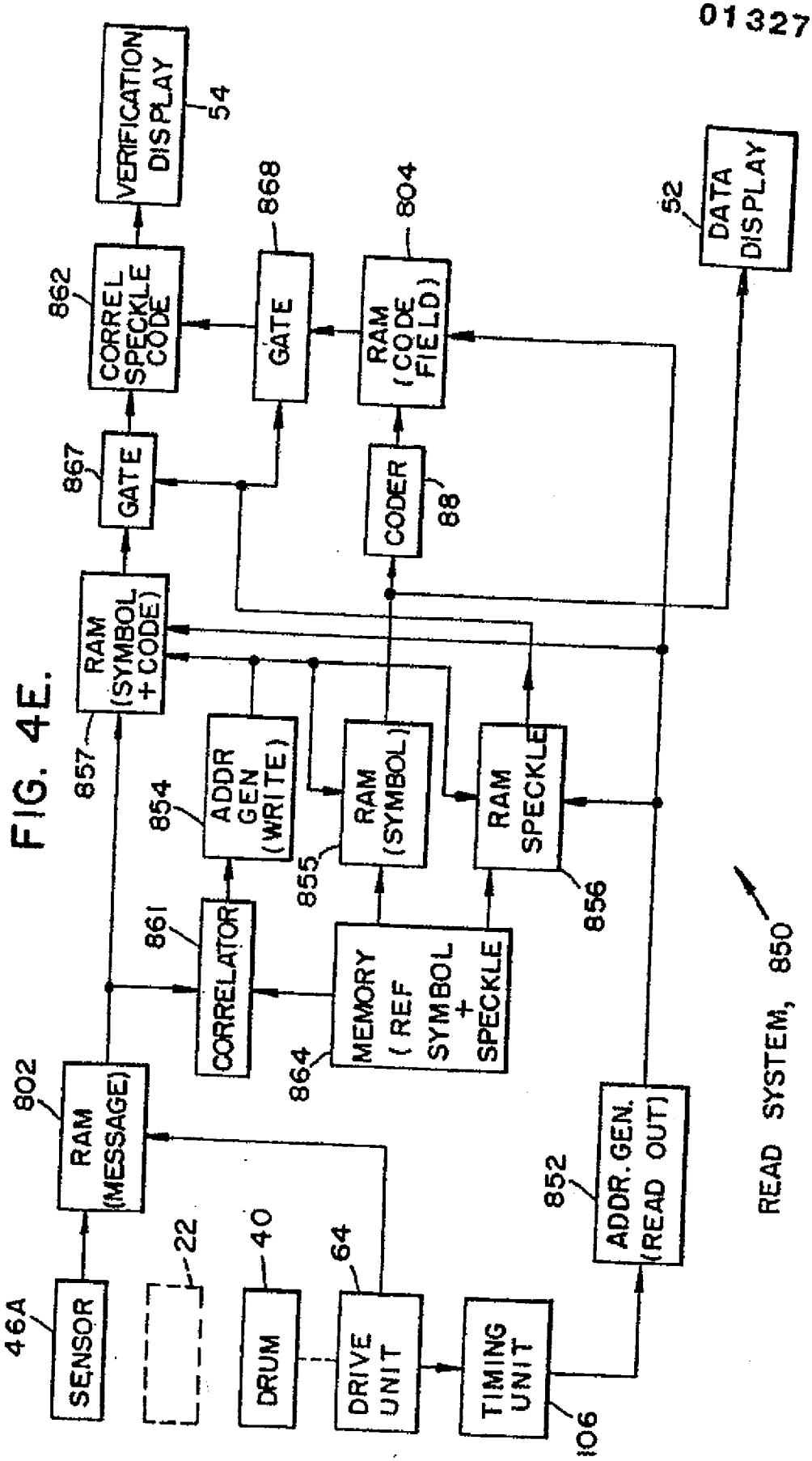

VERIFICATION DISPLAY
54
862
CORREL SPECKLE CODE
868
GATE
804
RAM (CODE FIELD)
52
DATA DISPLAY
867
GATE
CODER
88
857
RAM (SYMBOL + CODE)
854
ADDR GEN (WRITE)
855
RAM (SYMBOL)
RAM SPECKLE
856
861
CORRELATOR
MEMORY (REF SYMBOL + SPECKLE
864
802
RAM (MESSAGE)
852
ADDR. GEN. (READ OUT)
46A
SENSOR
22
40
DRUM
64
DRIVE UNIT
TIMING UNIT
106
READ SYSTEM, 850

FIG. 4E.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 154 972**
A2

EUROPEAN PATENT APPLICATION

(51) Int. Cl.⁴: G 07 D 7/00, G 07 B 17/00

(21) Application number: 85102784.7

(22) Date of filing: 12.03.85

(30) Priority: 12.03.84 US 588464

(43) Date of publication of application: 18.09.85
Bulletin 85/38

(84) Designated Contracting States: CH DE FR GB LI

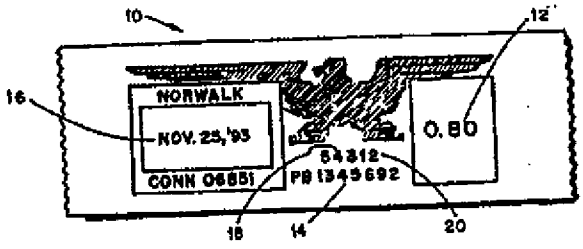
(71) Applicant: PITNEY BOWES, INC., Walter H. Wheeler, Jr. Drive, Stamford Connecticut 06926 (US)

(72) Inventor: Eckert, Alton B., 79 Tollsome Avenue, Norwalk, Conn. 06851 (US)

(74) Representative: Lehn, Werner, Dipl.-Ing. et al, Hoffmann, Eitle & Partner Patentanwälte Arabellastrasse 4 (Sternhaus), D-8000 München 81 (DE)

(54) **Method and apparatus for verifying postage.**

(57) An indicia (10) having an encrypted mark (20) is stamped upon a mail piece to represent postage so as to provide a code for authentication of such postage.



EP 0 154 972 A2

METHOD AND APPARATUS FOR VERIFYING POSTAGE

The present invention relates to a method and apparatus for verifying postage.

Postage meters find extensive use throughout the world for imprinting postage on objects to be mailed. Postage, of course, is the amount of money or fee required to have the Post Office deliver a mail piece to which the postage is applied to an indicated address. The postage may be applied to a mail piece by a print head enclosed within the postage meter, i.e., directly upon an envelope or upon a label. When postage is printed upon a label, the label is then placed in adhering contact onto an envelope, parcel or other object to be mailed. The postage meter is also capable of printing information in addition to the amount of postage. For example, the postage meter is used for imprinting the date of mailing, the piece number, suitable indicia designating instructions and/or routing information for transport by private carriers, and the like as is well known. Furthermore, if desired, the postage meter can be utilized for the imprinting of yet other forms of labels, such as tax stamps, assuming that governmental approval for such tax stamps is obtained.

A potential problem in the use of imprinted postage is the attempt at fraudulent adulteration of such postage; whereby, in effect, the person adulterating the postage is stealing the value of the postage. A fraudulent impression may enable someone to obtain postage, or in the case of a tax stamp, to avoid paying the tax. The foregoing problems have been overcome by various methods of determining if the postage on a mail piece is genuine through various forms of encryption and apparatus have been designed to implement such methods.

The instant invention provides an advantageous method and apparatus for determining if the postage on a mail piece is genuine. The apparatus includes electronic circuitry for the development of an encrypted mark, and a printer which is driven by the electronic circuitry to imprint an indicia with both the postage and other information in combination with an encrypted mark. The encrypted mark may be in the form of alphanumeric characters or other printwork and may be used for verifying the postage. An important feature of the invention is that encryption derived from data on the mail piece such as the amount of postage, the date, and, if desired, the sender and other data; thereby, the data imprinted on the mail piece or label is related to the encrypted mark. In the event that the printed matter is altered, either the encrypted mark cannot be decoded or, if decoded, the postage will not agree with the encrypted mark imprinted on the mail piece.

For a better understanding of the invention, and to show how the same may be carried into effect, reference will now be made, by way of example, to the accompanying drawings in which:

Fig. 1 shows a typical indicia imprinted by a postage meter upon a label, and

Fig. 2 is a block diagram describing the features of the invention.

Referring now to Fig. 1, a standard indicia that is imprinted by a postage meter on a mail piece is shown generally at 10. The indicia includes the amount of postage 12, a meter number 14 that identifies the postage meter that printed the indicia, the date 16 the postage is printed, the piece count 18, that indicates the number of times the postage meter has printed postage, and a code or encypted mark 20. In this embodiment, the encrypted mark 20 is in the form of numerics and is placed as if it were the least significant number of the piece count 18. It will be

appreciated that the encrypted mark 20 may be in the form of alphanumerics, and that the encrypted mark may be placed anywhere whether in the form of numerics, alphanumerics or any similar type of mark.

Coders for obtaining an encrypted mark 20 are well known and may use a variety of systems such as that used by the National Bureau of Standards based on the multiplication of pairs of large numbers. A coder that may be utilized in the instant invention for obtaining a seed number and a resulting encrypted mark is described in European Patent Application, No. 84 108 485.8 (US Serial No. 515,760 assigned to the assignee of this application) the disclosure of which is hereby incorporated by reference.

In Fig. 2, a system is shown that may be utilized to validate the information shown in Fig. 1., and includes a decoder 22. This decoder may be a microprocessor such as an Intel model 8039. When there is a question as to the validity of the postage on a mail piece, a postal official, or clerk, would input into the decoder 22 the postage amount 12, the serial number 14, the date 16, the piece count 18 in any convenient manner. The decoder 22 would have resident therein the seed number generated by a coder. The decoder is utilized for decoding and performs an encryption algorithm for determining the valid encryption mark based upon information supplied to the decoder. After processing the input information, the valid mark would be supplied to the postal official, as for example, on a display. If the mark generated by the decoder 20 corresponds to the number following the piece count, than the operator knows the postage is genuine. If there is no such match, then the postal official is aware of wrongdoing and can take appropriate action.

As stated previously, the encrypted mark 20 may be placed at any appropriate part of the indicia in any convenient form. For example, the encrypted mark 20 could be a part of the postage meter number or it could stand alone. In any event, as long as a standard system is established in accordance with the teachings herein, the authenticity of postage may be verified.

CLAIMS:

1. A method of verifying postage through an encrypted mark (20) that is part of an indicia (10) applied to a mail piece, characterized by:

providing a decoder (22) having a seed number stored in memory;

inputting data selected from information of the indicia (10);

deriving an encrypted message from the decoder based upon the stored seed number and input data; and

comparing an encrypted message generated by the decoder (22) against the encrypted mark (20) on the mail piece.

2. A method according to claim 1, characterized by the step of providing the postage fee (12), the meter serial number (14), the piece count (18) and the data (16) as part of the input data.

3. Apparatus for verifying postage, characterized by:

encryption means (22) for generating an encrypted mark (20);

means for supplying information relating to data printed (10) on a mail piece to said encryption means (22); and

means for indicating said encrypted mark.

4. Apparatus for verifying postage, characterized by:

encryption means for generating an encrypted mark;

means for supplying information relating to data printed on a mail piece to said encryption means; ar

means for printing said encrypted mark on said mail piece.

5. Apparatus according to claim 3 or 4, including means for generating a seed number as part of said encryption means (22).

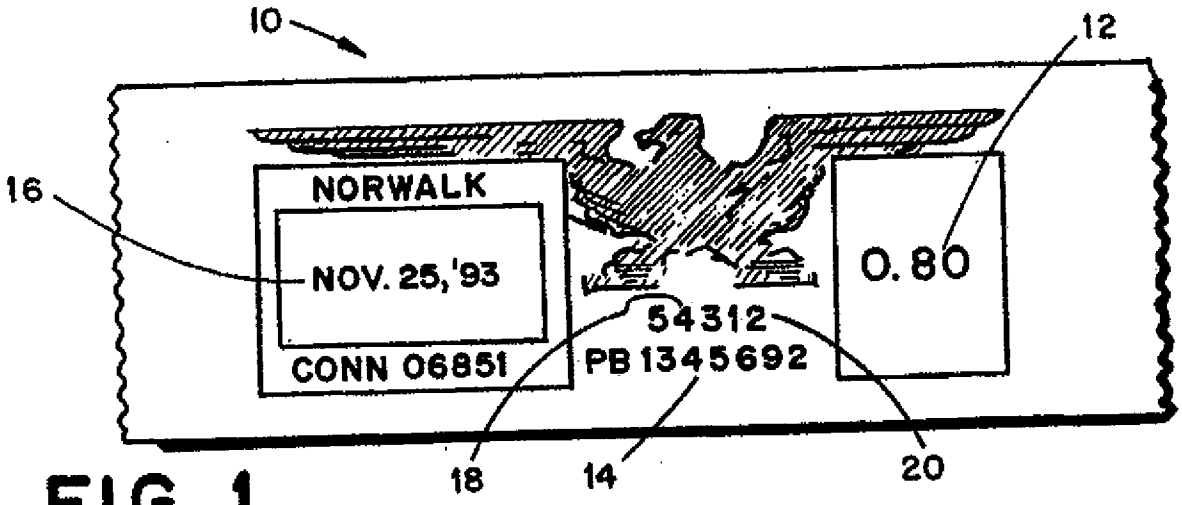

10
12
16
NORWALK
NOV. 25,'93
CONN 06851
0.80
54312
PB 1345692
18
14
20

FIG. 1

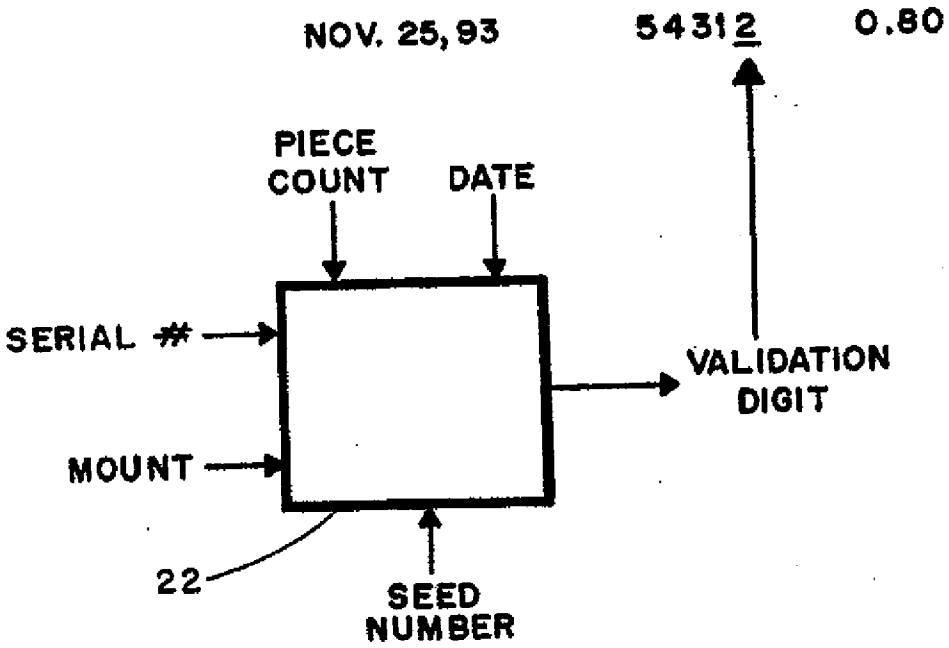

NOV. 25, 93
54312
0.80
PIECE COUNT
DATE
SERIAL #
MOUNT
VALIDATION DIGIT
22
SEED NUMBER

FIG. 2

(19) European Patent Office
Office européen des brevets

(11) Publication number: 0 331 352 A2

EUROPEAN PATENT APPLICATION

(12)

(21) Application number: 89301776.4

(51) Int. Cl.4: G07B 17/02

(22) Date of filing: 23.02.89

(30) Priority: 29.02.88 GB 8804689

(43) Date of publication of application:
06.09.89 Bulletin 89/36

(84) Designated Contracting States:
AT BE CH DE ES FR GB IT LI NL SE

(71) Applicant: ALCATEL BUSINESS SYSTEMS LIMITED
P.O. Box 3 South Street
Romford Essex, RM1 2AR(GB)

(84) DE FR GB

Applicant: ALCATEL N.V.
Strawinskylaan 537 (World Trade Center)
NL-1077 XX Amsterdam(NL)

(84) BE CH ES IT LI NL SE AT

(72) Inventor: Gilham, Dennis Thomas
12 Larkin Close
Brentwood Essex CM13 2SL(GB)

(74) Representative: Loughrey, Richard Vivian Patrick et al
HUGHES CLARK & CO 63 Lincoln's Inn Fields
London WC2A 3JU(GB)

(54) Franking system.

(57) A method of franking mail items (10) is disclosed in which the franking impression includes a machine readable portion (12) and a visually readable portion (11). The machine readable portion (12) comprises a data block including at least a postage charge and a pseudo-random number and the data block is encrypted prior to printing. During printing of the franking impression, at least a part of the machine readable portion (12) is read (17) and compared with the data block intended to be printed. If the comparison is satisfactory the printing operation is continued to print the visually readable portion (11). The pseudo-random number is changed for each franking transaction which may be each item or batch of items. The machine readable portion is read at a mail handling centre to provide an input to a postage charging and accounting function.

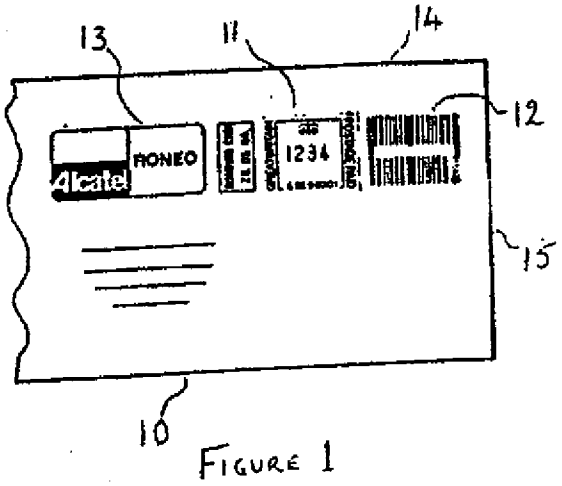


FIGURE 1

EP 0 331 352 A2

FRANKING SYSTEM

This invention relates to a method of franking postal items by which postal authorities are enabled to account for charges relating to the handling of mail items and to obtain payment for such charges from the sender of the mail items. The invention also relates to franking apparatus for carrying out the method.

Currently used postage payment systems for franking machines fall into two categories. In one category, in which the postage is prepaid, the franking machine is constructed and operated to securely maintain a record of credit remaining available to a user of the machine and the machine is controlled to lock if and when the credit level decreases to a predetermined low value. Consequently if this low credit level is reached and the machine locks, the machine is unable to be used for further franking until such time as payment has been received by the postal authority for additional credit and the new credit value has been entered in the machine. In the other category in which a post payment method is used, the meter is read periodically and the user invoiced accordingly, use of the franking machine is constrained by controls which lock the machine when total postage value used exceeds a predetermined limit. In both of these categories of system it is necessary for the franking machine to incorporate security measures to prevent fraudulent use of the machine. In order to maintain the integrity of the security complex control systems are used in the internal operation of the machine and the franking machine is constructed to be physically robust and is provided with sealing devices to prevent unauthorised access to the interior of the machine. In addition to the security maintained in the franking machine, the postal authorities operate an elaborate manual procedure for checking franked mail items which necessitates restriction of location at which franked mail can be posted by any sender. The maintenance of security in the franking machine increases the cost of the franking machine and this together with restrictive posting procedures tends to limit the use of franking machines to those users which have a relatively large volume of postal usage.

Broadly the invention relates to a system of franking mail items comprising printing franking data in machine readable form on said mail items by senders of said items, said franking data including at least data relating to a postage charge for the item encoded in a secure manner to prevent unauthorised printing of said data relating to the postal charge and identification data; utilising a data reading device to read said imprinted franking data from the mail items at a postal authority location to provide data signals relating to each mail item; utilising said data signals to generate a transaction record for each of the franked items and utilising said transaction records to generate a billing account for each sender of franked mail items.

According to one aspect of the invention a method of franking mail items comprises the steps of generating a pseudo-random number relating to a franking transaction; forming a data block containing at least said pseudo random number and data relating to a postal charge for said mail item; encrypting said data block; printing data representing said encrypted data block together with identification data in machine readable form on a mail item.

Preferably a different pseudo random number is generated for each franking transaction.

The franking data may be printed on the mail item in the form of a bar code consisting of spaced bar code marks of differing width.

According to another aspect of the invention a method of franking mail items and accounting for postage value used comprises at a mail item franking location the steps of generating a pseudo-random number relating to a franking transaction; forming a data block containing at least said pseudo random number and data relating to a postal charge for said mail item; utilising an encryption key unique to a franking machine to encrypt said data block; printing data representing said encrypted data block together with data identifying said franking machine in machine readable form on a mail item; and at a postal authority location the steps of machine reading said identification data and printed encrypted data block; selecting from a record of decryption keys a decryption key corresponding to said identification data; utilising said selected decryption key to decrypt said encrypted data block read from the mail item; checking validity of the pseudo-random number contained in said data block and if valid utilising the postage charge data as an accounting input to account for postage value used.

Preferably a record of pseudo random numbers used in relation to a franking machine identification is maintained; a pseudo random number read from franking data of a current mail item is compared with the record of pseudo random numbers; and the franked mail item is accepted for despatch to a destination address only if said pseudo random number is valid.

In accordance with yet another aspect of the invention franking apparatus includes means to

generate a pseudo random number for each franking transaction; means to form a data block by combining said pseudo random number with a postal value selected for franking a mail item; and printing means operable to print franking data including said data block in machine readable form on the mail item.

Preferably the franking apparatus includes means operable in combination with a secure encryption key to encrypt said data block.

Preferably the franking apparatus includes reading means operative to read said franking data printed in machine readable form on the mail item; and means operative to compare franking data intended to be printed with the franking data read by said reading device and to terminate franking in the event that the comparison means indicates an error in the printed franking data.

The franking apparatus may include means operable to print a visually readable franking on the mail item only if the comparison means indicates that the printed franking data is free of error.

A method of and apparatus for carrying out the invention will now be described by way of example with reference to the drawings in which:-

Figure 1 shows a franking impression on a mail item

Figure 2 is a flow diagram of the operation of a franking machine

Figure 3 is a flow diagram of procedures carried out at a postal authority centre and

Figure 4 is a block diagram of franking apparatus.

Referring first to Figure 1, a franking printed onto a mail item 10 comprises two parts indicated as 11 and 12. The part 11 consists of a typical franking such as is applied by current franking machines to enable visual inspection of a mail item to ascertain that it has been correctly franked with a value of postage appropriate to the size or weight of the item, the destination of the item and the postal service such as surface mail or airmail required by the sender. The franking consists of a predetermined pattern as governed by rules laid down by the postal authority and usually includes not only the value of postage but also the date of franking and the licence number of the franking machine. At the time of printing the franking additional information such as a slogan 13 may be printed on the mail item alongside the franking. In addition the franking impression includes the portion 12 consisting of an impression in a coded form which can be read by machine. The coded impression may take a number of forms, the form illustrated consisting of a bar code in which data is represented in binary notation by spaced bars of one or other of two widths. In printing the franking, it is usual for the mail item, an envelope in this present example, to be fed in a direction left to right as seen in Figure 1 in which the upper edge 14 engages and is guided by a guide on the franking machine and the right hand edge 15 is the leading edge of the envelope. These edges 14 and 15 of the mail item serve as datum edges for the positioning of the franking impression on the item. The bars of the bar code, in the portion 12 of the franking, extend transversely to the direction of feeding of the mail item and are spaced apart in the direction of feeding of the mail item. The portion 12 may consist of a single row of bars or where the quantity of data to be represented would require an unduly long row of bars, the data may be represented by bars arranged in a number of rows, for example two rows, as shown in Figure 1. It will be appreciated that instead of printing directly onto the envelope, the mail item on which printing is effected may comprise an adhesive label for subsequent application to an envelope or parcel. Conveniently, the franking may be printed by a thermal print head 16 (Figure 4) which has a plurality of print elements disposed along a line extending transversely to the direction of feeding of the mail item. The print elements are selectively energised in synchronism with the feeding of the mail item in such a manner as to achieve printing of the required franking impression. Since the portion 12 consisting of coded data is required to be read by machine it is desirable to check the printing of the bar code by a reading device 17 positioned upstream and immediately adjacent the print head. The data represented by the bar code in the portion 12 of the franking impression includes date of franking, postage value and franking machine identification which conveniently may be the licence number of the franking machine. In addition it is preferred to include the despatch postal area code and the destination postal code. In order to ensure that the data, particularly that relating to the postage value, is valid and is secure from attempts to fraudulently print or tamper with that data, the data is formed into a secure code or data block. This is effected by causing the franking machine to generate a pseudo random number and to combine this with at least the postal value to form a data block. This data block is then encrypted using a secure encryption key held in non-volatile memory in the franking machine. The licence number of the franking machine and the despatch and destination areas codes are combined with the secure data block after encryption. The pseudo random numbers are generated in a sequence so that successive numbers of the sequence are used for each franking transaction. A franking transaction may comprise franking of an individual mail item or may comprise franking of all mail items during a pre-

determined time period, for example one day. Thus, in the latter instance, the pseudo random number is reset for each day and this may be effected by an algorithm triggered by resetting the date in the franking machine. Thus the data block for each franking transaction is unique. As will be seen from Figure 4, the franking machine includes electronic circuits 18 operable to control operation of the print head 16 and to receive output signals from the reading device 17. Non-volatile memory 19 is provided to store the licence number of the franking machine and any other data which may be required in the operation of the machine. The circuits 18 are operable under the control of software programs to generate pseudo random numbers in sequence and to form a data block by combining a postage charge value input on a keyboard 20, or from another source, and to utilise an encryption key held in a secure location of memory 19 to encrypt the data block and then carry out a printing operation in which franking data including the encrypted data block is printed in the form of a bar code on the mail item fed past the print head 16.

Figure 2 illustrates steps in the franking machine operation from which it will be seen that after encryption of the data block, the portion 12 of the franking impression is printed and, immediately thereafter, is read by the reading device. The output of the reading device is compared with the data block intended to be printed. If the comparison indicates that the printed bar code correctly represents the data block, the operation of the franking machine continues so as to print the visually readable portion 11 of the franking impression and the mail item 10 bearing a complete franking impression 11, 12 and, where desired, a slogan or the like 13 is fed from the franking machine. However if the comparison indicates that the data block is not correctly represented by the printing, printing of the remainder of the franking impression is terminated and a fault message is displayed on the franking machine. The output of the reading device in respect of the whole of the portion 12 of the franking impression may be compared with the whole of the data block intended to be printed. However the processing of the data in the comparison operation may take a length of time such that a pause would be required before continuing after a correct comparison to print the visually readable portion 11 of the franking impression. In order to enable the printing of the entire franking impression to be continuous and uninterrupted, the comparison may be carried out on a probability basis and be in respect of only a leading part of the portion 12 of the franking impression. If a comparison in respect of this part of the portion 12 indicates that this part is correct, a decision would be made to continue printing and the visually readable portion would be printed immediately following printing of the machine readable portion in a continuous printing operation. While such a partial comparison would not check the entire portion 12, on a probability basis, if this part has been correctly printed by the printing device, the printing device will continue to function correctly to print the remainder of the portion 12 and the partial comparison will provide an adequate and sufficient check of the printing.

The postage value and destination code are input to the franking machine by the user, or from another station in a mailing system of which the franking machine is a part. The date of franking may be set automatically from a clock device in the franking machine and the licence number is read from a location of non-volatile memory where it is stored.

The licence numbers and corresponding users secure encryption keys are held in a data base accessible by mail handling apparatus at a postal authority location. Referring to Figure 3, when the franked mail item 10 is received at the postal authority location, it is fed into an automatic mail handling apparatus. The apparatus includes a suitable code reader for reading the bar code of the portion 12 of the franking impression. Upon reading the licence number from the portion 12 of the franking impression, the data base is accessed to obtain the secure encryption key associated with that licence number and the key is utilised to decrypt the secure data block represented by the bar code of portion 12 of the franking impression. Validation checks are carried out on the data within the block to check validity of the data. The validity checks include a check to ensure that the data read from the secure block is error free, a check on the pseudo random number to ensure that it is a valid current pseudo random number, a check that the licence number of the machine relates to a current account with the postal authority and a check that the date and value of franking have allowable values. If the validation checks indicate that the coded franking impression is valid and acceptable by the postal authority the mail item is fed for sorting and handling in the usual manner. If the portion 12 of the franking impression includes destination data for the mail item, reading of this destination data by the code reader may be utilised to control mechanical sorting apparatus to direct the mail item to an appropriate destination area bin. In the event that either the reading of the code portion 12 indicates a faulty reading of the data or the validity check on data in the secure data block indicates that the data is not valid, the mail item is directed to a station where a manual check of the franking impression can be effected. If, from the manual check, the franking impression is judged to be valid the franking and destination details are

entered manually at a keyboard terminal and the item is re-introduced into the mechanical handling system. On the other hand, if it appears that the franking impression is invalid and possibly results from an attempted fraudulent action, the mail item may be passed to a supervisor for attention. The franking data read from the portion 12 of the franking impression and after decryption of the secure data block, together with similar franking data entered manually on the keyboard terminal is utilised to enter the postal charge for the mail item as a transaction on a computerised accounting system. Billing of users of the franking machines may be effected from the accounting system and in addition reports concerning usage of the mail handling system may be produced for management and other purposes.

Claims

1. A method of franking mail items characterised by the steps of generating a pseudo-random number relating to a franking transaction; forming a data block containing at least said pseudo random number and data relating to a postal charge for said mail item; encrypting said data block; printing data (12) representing said encrypted data block together with identification data in machine readable form on a mail item (10).

2. A method as claimed in claim 1 further characterised by the steps of machine reading said printed data (12) from said mail item (10); comparing information obtained from reading said printed data block with information contained in said data block and in response to identity therebetween printing a visually readable franking impression (11) including at least a postage charge on the mail item.

3. A method as claimed in claim 2 further characterised in that the step of comparing is effected in respect of only a part of the information obtained from reading said printed data block (12).

4. A method as claimed in claim 2 further characterised in that the step of comparing is effected in respect of the whole of the information obtained from reading said printed data block (12).

5. A method as claimed in any preceding claim further characterised by the step of generating for each of a series of franking transactions respectively a next pseudo-random number of a series of pseudo-random numbers.

6. A method as claimed in claim 5 further characterised in that a franking transaction comprises franking of a single mail item (10) and wherein the next pseudo-random number of the series is generated for the franking of each successive mail item.

7. A method as claimed in claim 5 further characterised in that a franking transaction comprises franking of a batch comprising a plurality of mail items (10) and wherein the next pseudo-random number of the series is generated for the franking of a first mail item of each successive batch of mail items.

8. A method as claimed in claim 7 further characterised by the steps of registering a current date and generating the next pseudo-random number of the series in response to change in the registered date.

9. A method of franking mail items and accounting for postage value used characterised by, at a mail item franking location, the steps of generating a pseudo-random number relating to a franking transaction; forming a data block containing at least said pseudo random number and data relating to a postal charge for said mail item; utilising an encryption key unique to a franking machine to encrypt said data block; printing data representing said encrypted data block together with data identifying said franking machine in machine readable form (12) on a mail item (10); and, at a postal authority location, the steps of machine reading said identification data and printed encrypted data block (12); selecting from a record of decryption keys a decryption key corresponding to said identification data; utilising said selected decryption key to decrypt said encrypted data block read from the mail item (10); checking validity of the pseudo-random number contained in said data block and if valid utilising the postage charge data as an accounting input to account for postage value used.

10. A method as claimed in claim 9 further characterised by the step, at the postal authority location, of maintaining a record of pseudo-random numbers used in franking mail items (10) at the franking location corresponding to the identification data; and comparing the pseudo-random number from the data block read from the mail item with pseudo-random numbers already used at that franking location and accepting the mail item as validly franked if the pseudo-random number has not been used.

11. A method of franking a mail item characterised by the steps of generating a different pseudo-random number for each franking transaction; printing on the mail item (10) franking data in machine readable form (12), said franking data including a data block containing data relating to a postal charge for said item and the pseudo-random number applicable to that mail item, said data block being encrypted prior to printing on the mail item.

12. A method of handling a mail item franked by a method as claimed in any preceding claim characterised by the steps of utilising a reading

device (17) to read the franking data (12) printed on the mail item (10)in machine readable form; maintaining a record of pseudo random numbers used in relation to a franking machine identification; comparing a pseudo random number read from franking data of a current mail item with the record of pseudo random numbers; accepting the franked mail item for despatch to a destination address only if said pseudo random number is not included in said record and adding the pseudo-random number of the franking data of the current item to said record of pseudo-random numbers.

13. Franking apparatus characterised by means (18) to generate a pseudo random number for each franking transaction; means (18) to form a data block by combining said pseudo random number with a postal value selected for franking a mail item; and printing means (16) operable to print franking data including said data block in machine readable form (12) on the mail item (10).

14. Franking apparatus as claimed in claim 13 further characterised by means (18) operable in combination with a secure encryption key to encrypt said data block prior to printing on the mail item (10).

15. Franking apparatus as claimed in claim 13 or 14 further characterised by reading means (17) operative to read said franking data printed in machine readable form (12) on the mail item (10); and means (18) operative to compare franking data intended to be printed with the franking data read by said reading device (17) and to terminate franking in the event that the comparison indicates an error in the printed franking data.

16. Franking apparatus as claimed in claim 15 further characterised in that the printing means (16) is operative to print visually readable franking (11) on the mail item (10) only if the comparison indicates that the printed franking data (12) is free of error.

17. Franking apparatus as claimed in claim 16 further characterised in that the printing means (16) is operative to print a visually readable franking (11) including at least a visually readable postage value.

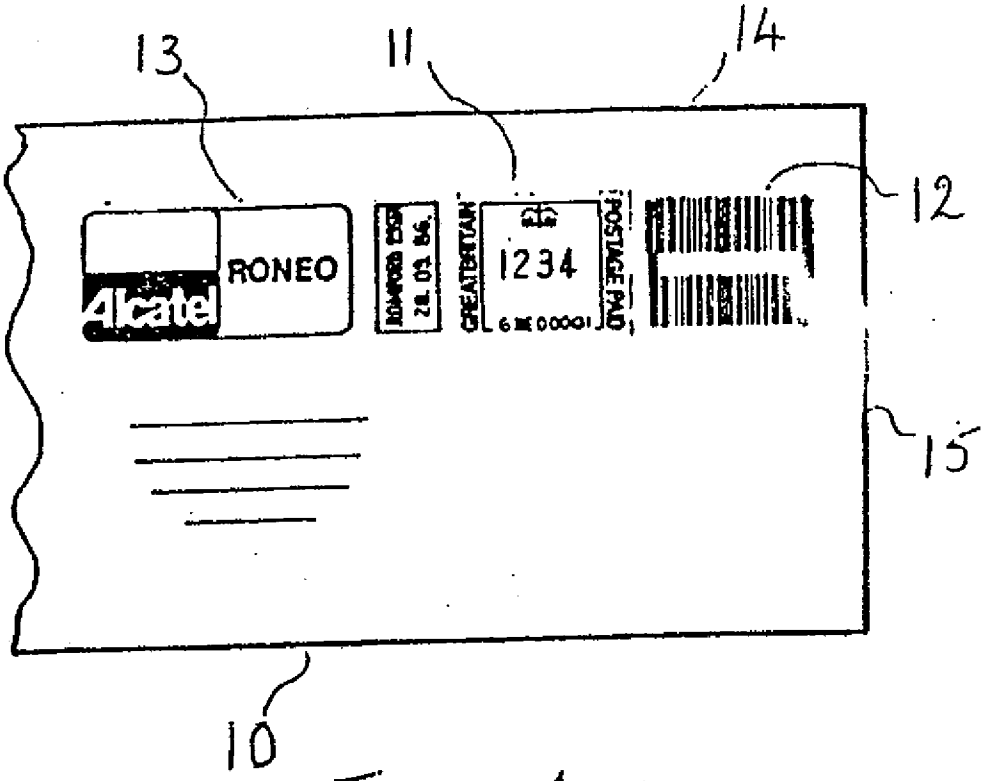


FIGURE 1

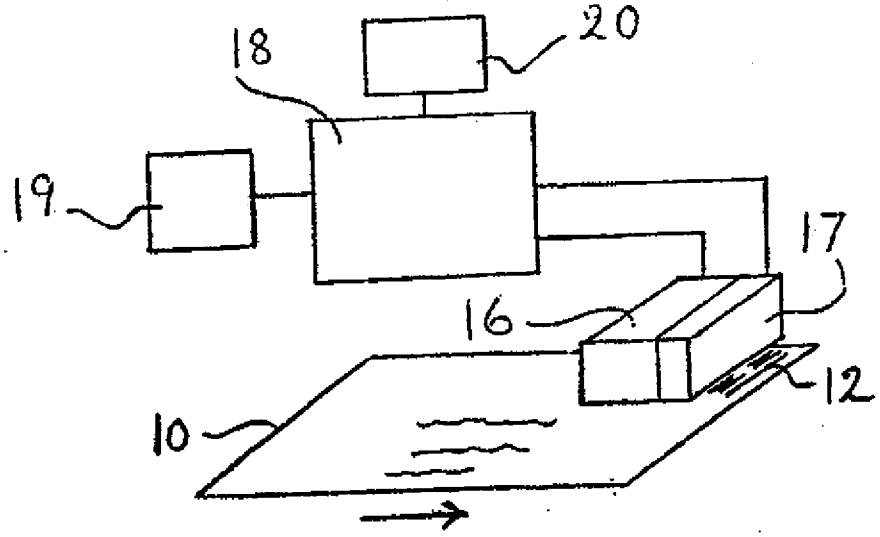


FIGURE 4

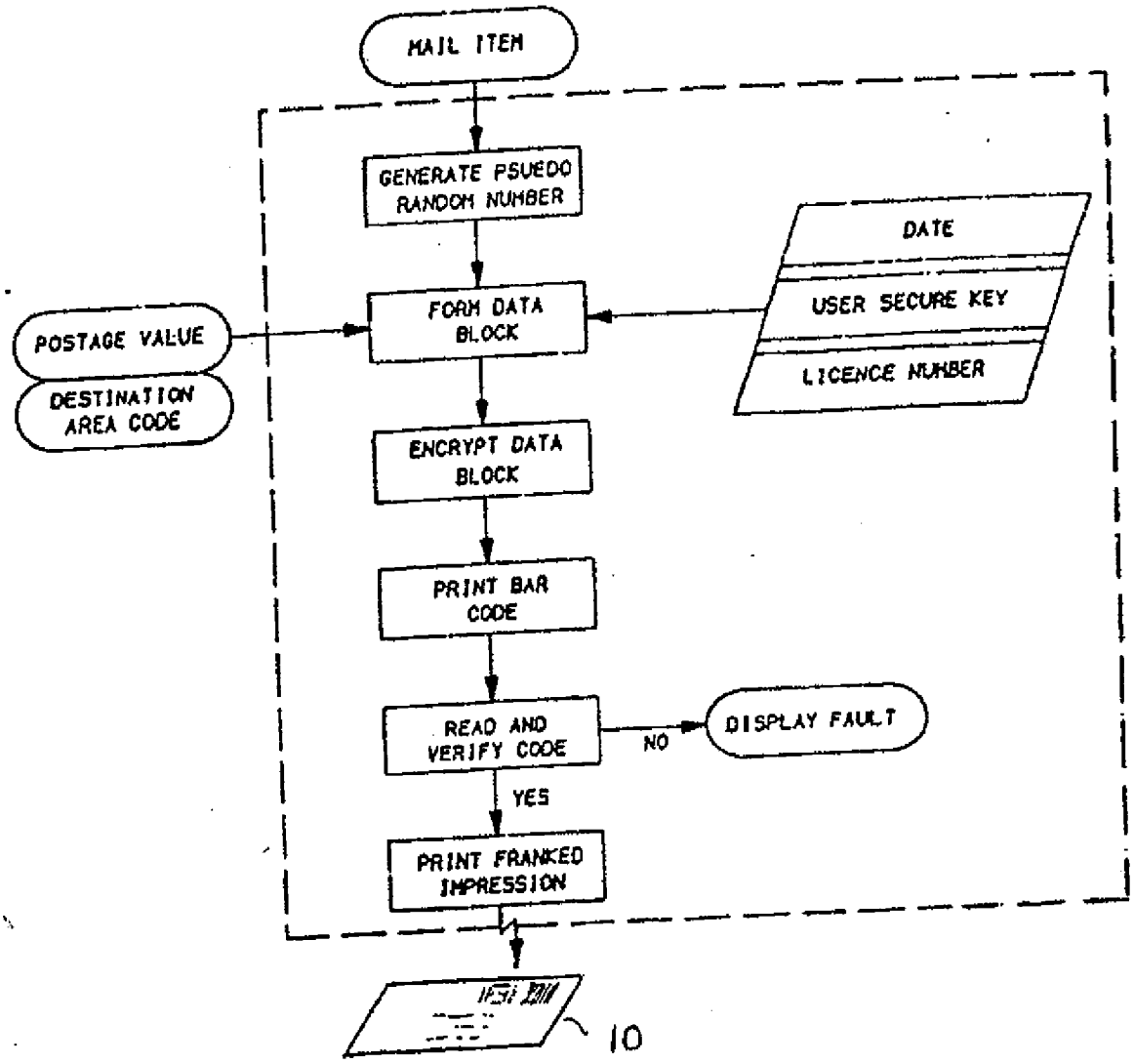

MAIL ITEM
GENERATE PSUEDO RANDOM NUMBER
DATE
USER SECURE KEY
LICENCE NUMBER
POSTAGE VALUE
DESTINATION AREA CODE
FORM DATA BLOCK
ENCRYPT DATA BLOCK
PRINT BAR CODE
READ AND VERIFY CODE
NO
DISPLAY FAULT
YES
PRINT FRANKED IMPRESSION
10

FIGURE 2

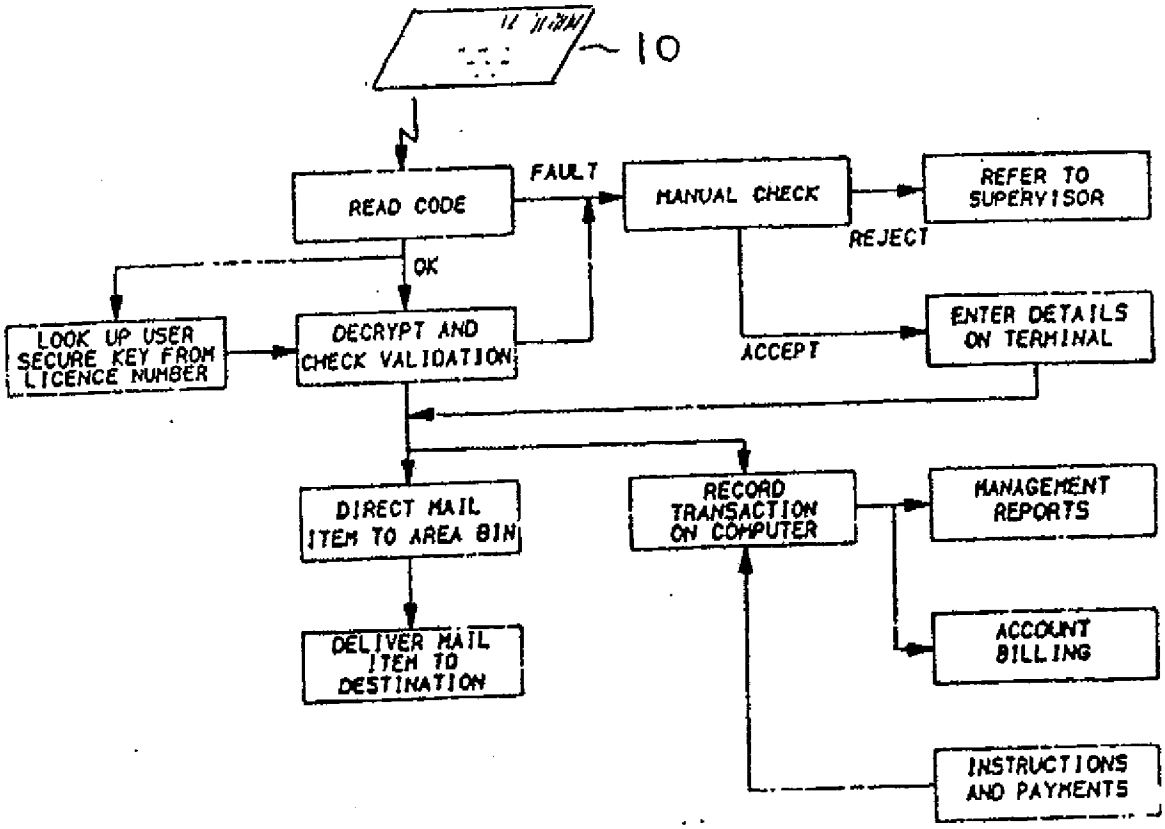

10
READ CODE
FAULT
MANUAL CHECK
REFER TO SUPERVISOR
REJECT
OK
LOOK UP USER SECURE KEY FROM LICENCE NUMBER
DECRYPT AND CHECK VALIDATION
ACCEPT
ENTER DETAILS ON TERMINAL
DIRECT MAIL ITEM TO AREA BIN
RECORD TRANSACTION ON COMPUTER
MANAGEMENT REPORTS
ACCOUNT BILLING
DELIVER MAIL ITEM TO DESTINATION
INSTRUCTIONS AND PAYMENTS

FIGURE 3

K

008727324 **Image available**
WPI Acc No: 91-231339/199132
XRPX Acc No: N91-176343

Franking machine identification - using machine data combined with data and valve of franking in coded identification

Patent Assignee: FRANCOTYP-POSTALIA (FRAN-N); FRANCOTYP POSTALIA GMBH (FRAN-N)
Inventor: DIETRICH K

Number of Countries: 006 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
DE 4003006	A	19910801	DE 4003006	A	19900130		199132 B
EP 440021	A	19910807	EP 91100186	A	19910108		199132
US 5186498	A	19930216	US 91647442	A	19910129	B42D-015/00	199309
EP 440021	A3	19920122	EP 91100186	A	19910108		199322
DE 4003006	C2	19930812	DE 4003006	A	19900130	G07B-017/04	199332
EP 440021	B1	19941026	EP 91100186	A	19910108	G07B-017/04	199441
DE 59103303	G	19941201	DE 503303	A	19910108	G07B-017/04	199502
			EP 91100186	A	19910108	E	

Priority Applications (No Type Date): DE 4003006 A 19900130
Cited Patents: NoSR.Pub; EP 331352; EP 352498; GB 2173741; GB 2193157; GB 2193468
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
EP 440021	A					
Designated States (Regional): CH DE FR GB LI						
US 5186498	A		4			
DE 4003006	C2		4			
EP 440021	B1	G	5			
Designated States (Regional): CH DE FR GB LI						
DE 59103303	G			Based on		EP 440021

Abstract (Basic): DE 4003006 A

A microprocessor controlled franking machine establishes an identification characteristic that contains data defining the data and machine type in a form that cannot be falsified.

The system uses a machine parameter (MP), date (DT) and franking value (WE) that are combined in a coding algorithm (KA). The resulting output is a multidigital coded value that is printed.

ADVANTAGE - Coded identification is protected against falsification.

Dwg.1/2

Title Terms: FRANKING; MACHINE; IDENTIFY; MACHINE; DATA; COMBINATION; DATA; VALVE; FRANKING; CODE; IDENTIFY
Derwent Class: P76; T01; T05
International Patent Class (Main): B42D-015/00; G07B-017/04
File Segment: EPI; EngPI

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 526 166 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 92306883.7

(51) Int. Cl.5: G06F 15/42

(22) Date of filing: 28.07.92

(30) Priority: 29.07.91 US 737351

(43) Date of publication of application:
03.02.93 Bulletin 93/05

(84) Designated Contracting States:
AT BE CH DE FR GB LI NL SE

(71) Applicant: Dessertine, Albert L.
53 Park Avenue
Flemington, New Jersey 08822(US)

(72) Inventor: Dessertine, Albert L.
53 Park Avenue
Flemington, New Jersey 08822(US)

(74) Representative: Ablewhite, Alan James
MARKS & CLERK 57/60 Lincoln's Inn Fields
London WC2A 3LS(GB)

(54) Patient compliance monitoring method and system.

(57) The present invention is directed to a method of monitoring a patient's medicine compliance. It involves utilizing an automatic compliance monitoring device which tracks patient compliance data, along with a wave energy transmitter and power source, all connected to a medicine container. A receiver is connected to a computer with a display unit. The compliance monitoring device or the computer is programmed to calculate compliance requirements of the container e.g. by number of cap openings, by dispensing count or by weight information obtained by the automatic compliance monitoring device, for each dosage administration for the prescription period. The wave energy transmitter on the medicine container continuously, periodically, or randomly transmits raw or calculated data to the receiver and from there to the computer to compare actual usage with compliance required, to determine compliance results on the display unit to permit compliance monitoring on a monitor at a remote location. Optionally, other patient characteristics are also monitored and feedback is provided. The present invention includes both the method and the system of interconnected devices to practice the method as well as a single component which includes in combination, the medicine container, compliance device, transmitter and power source. Feedback may be to any professional or any remote location, and a single medicine or a plurality of medicines may be monitored.

EP 0 526 166 A2

The present invention is directed to a method, system and component for monitoring a patient's compliance with a medicine regimen. It is directed to compliance monitoring by another person other than the patient, such as a relative or a professional such as a pharmacist, doctor, hospital, clinic or the like, at a location remote from the patient. The present invention involves the use of one or more automated compliance monitoring devices, wave energy transmitters, remote receivers and computers for monitoring and optionally includes monitoring of other patient status information such as physical characteristics, e.g. heart rate, blood pressure, etc. and/or treatment program compliance such as physical therapy or exercise regimens.

The use of precision, automatic compliance monitoring devices, unique programming and remote radio transmission of data directly from the medicine containers to computers and linking peripherals to monitor medicine regimen compliance has not been taught in the prior art.

U.S. Pat. No. 4,577,710 issued to Edward Ruzumno is directed to an apparatus for promoting good health which involves a personal weight scale and an information and message center which may be used merely for weight control or may be used for specific messages pertaining to a health condition with pre-taped feedback from a physician. This recently issued patent represents the concept of patient weight monitoring for general or specific health purposes. However, it does not pertain to medicine regimen compliance, automatic compliance monitoring devices or computer linking as in the present invention.

Most recently, Time Magazine, June 5, 1989, at page 70 reported that Aprex, a California Company has developed a cap for use with medication containers. A computer chip in the cap records the day and time each time the cap is opened (for taking medicine). The professional, e.g. the doctor will, at a later time or visit, put the cap into an electronic analyzer that lets the user know how regularly the medicine was taken. This automatic compliance monitoring system, unfortunately, does not permit the doctor or pharmacy to monitor unless the cap is delivered to the analyzer.

U.S. Patent No. 4,899,839 issued to Dessertine and Hudson and assigned commonly to the assignee herein, describes a compliance system using a scale tied into a computer for weighing medicine containers and calculating usage, and, therefore, compliance, at specific or random times during a prescription period. This system requires the patient to physically place the medicine container on a scale and possibly perform other tasks related thereto.

U.S. Patent No. 5,016,172 to the inventor herein, Dessertine, and commonly assigned, describes compliance monitoring systems where the medicine container has a device for tracking (collecting, storing, retrieving) compliance data, and then inputting same by connecting the container to a computer, for compliance monitoring. Again, this requires some action on the part of the patient, e.g. plugging the computer and container together.

The present invention uniquely enables doctors, hospitals, pharmacies, manufacturers, data centers, etc. to monitor compliance from remote locations without requiring the patient to take any specific action not needed in the absence of compliance. In other words, the present invention is the first patient passive compliance monitoring method and system that provides the opportunity for ongoing feedback/information on the patient's compliance activity.

The present invention is directed to a method of monitoring a patient's medicine compliance. It involves utilizing an automatic compliance monitoring device which tracks patient compliance data, along with a transmitter and power source, all connected to a medicine container. A receiver is connected to a computer with a display unit. The compliance monitoring device or the computer is programmed to calculate compliance requirements of the container e.g. by number of cap openings, by dispensing count, by light band or intensity measurement, by weight information obtained by the automatic compliance monitoring device or the like, for each dosage administration for the prescription period. The radio transmitter on the medicine container continuously, periodically, or randomly transmits raw or calculated data to the receiver and from there to the computer to compare actual usage with compliance required, to determine compliance results on the display unit to permit compliance monitoring on a monitor at a remote location. Optionally, other patient characteristics are also monitored and feedback is provided. The present invention includes both the method and the system of interconnected devices to practice the method as well as a single component which includes in combination, the medicine container, compliance device, transmitter and power source. Feedback may be to any professional or any remote location, and a single medicine or a plurality of medicines may be monitored.

The present invention, its advantages and objects will be more fully understood when the specification herein is taken in conjunction with the drawings appended hereto, wherein:

Figure 1 illustrates a diagrammatic representation of some preferred embodiments of the present invention;

Figure 2 illustrates an alternative embodiment diagrammatic representation of the present invention;

Figure 3 illustrates a schematic diagram of the present invention showing the interrelationships of the various components; and,

Figure 4 shows an alternative embodiment schematic diagram of the present invention.

The present invention involves a method and a system for monitoring a patient's compliance with regard to adhering to a particular medicine regimen as well as a specific component involved in the system. It is directed to compliance monitoring by someone at a remote location, e.g. a relative or friend or paid service or by a professional such as a pharmacist, a doctor, a physical therapist, a chiropractor or the like or by a hospital or clinic or staff of a convalescence home or a remote data collection center, a government agency or other party or any combination of these. Thus, the present invention involves remote monitoring independent from the patient. Further, the invention involves using one or more automatic compliance monitoring devices, wave energy transmission, e.g. radio transmission, from the medicine container to a receiver and then, directly or indirectly, to one or more computers which are interconnected. In some embodiments the receiver may be located within the computer or attached integrally to it. In addition to medicine regimen, optional status of patient health characteristics may be monitored with computer tracking, feedback and other communication. Thus, a patient's heart rate, blood pressure, glucose level, cholesterol level, weight or other physical characteristics may be monitored or some compliance with a physical therapy program or exercise program may be monitored in addition to the medicine regimen monitoring.

By "medicine container" used herein is meant any portable container which may be carried by a patient and has a plurality of dosages of medicine. The medicine itself may be liquid, slurry, cream, paste, powder, capsule, caplet, tablet or any other dosage capable form. The medicine container will necessarily have a cap portion and a base portion. The "cap portion" may be a fully removable cap, a connected cap such as a hinged cap, or merely the door of an orifice. The "base portion" is the container minus the cap portion and is that part which holds the medicine.

The "automatic compliance monitoring device" described herein is meant to be any known or to be developed device connected to a medicine container - pill, capsule, liquid or otherwise - which tracks (recognizes and stores) data pertaining to actual medicine consumption or container usage. "Actual medicine consumption" means actual amount of medicine taken from a medicine container. Such devices may include cap opening counting devices such as the Aprex device described in the prior art above, or automatic pill counting devices or light band-based or light intensity-based contents measuring devices or weight or volume tracking devices connected to a container. It may be an optical scanner which measures volume or fill level or it may be another container-attached or attachable device. The details of the workings of such devices are now within the skill of the artisan and variations may be made without exceeding the scope of the invention.

The "transmitter" herein is a wave energy transmitter such as a radio or microwave transmitter, although no frequency limit to the transmission is intended. It has a power source for transmitting and may be capable of transmitting only short distances or long distances depending upon costs and purpose. For example, a transmitter in a medicine container for a hospital patient may need only a very short transmission with receivers in every room, on every floor or centrally located. Or, the user may have a transmitter at home or at work. The transmitter may be set up to transmit continuously, periodically or randomly, e.g in response to a stimulus. The transmitter may send unique identifiers and then compliance data, e.g. social security number of patient, medication code and pills removed , or weight, or fill level. The power source may be the same as one running the compliance device and may be, e.g. solar chargeable.

The receiver used may be any which will perform the function of receiving the data transmitted and forwarding it. The receiver may, for example,

(a.) forward the data directly to one or more computers;

(b.) pass the data through telephone lines or cable television lines to one or more data receiving computers at a more remote location;

(c.) pass the data to an amplifier, second transmitter where it may be retransmitted to a remote receiver directly or even via satellite to a regional, national or international data center;

(d.) simulcast the data by any or all of the above or any other available methods to diverse receivers, including conversion of data from radio to electronic, digital, sonic, optical or printed format;

(e.) in addition to, or separate from, any of the above, forward compliance or non-compliance information to a computer with a displayed message, e.g. with audio signal, to the patient to advise the patient to take some corrective action as needed. Likewise, unique computer display of problem compliance to a doctor, hospital, agency, etc. may be effectuated by the present invention method.

Referring now to Figure 1, there is shown a flow diagram with steps (A), (B) and (C) shown which involve preparing the system for using the method of the present invention as well as steps 1

through 4 which show an embodiment involving the steps of the present invention. Thus, frame 2 shows step (A) wherein an automatic compliance monitoring device, a wave energy transmitter, e.g. radio transmitter, and power source are attached to a medicine container. The frequency of the wave energy transmitter is not critical as long as the wave energy is sent and received in useable form. Low, high, ultrahigh, microwave, C-band, Ku-band or any available frequency may be used.

Frame 4 indicates in step (B) that, separately, a receiver, computer and display unit are provided. Thus, any automatic compliance monitoring device which is capable of accurately, electronically determining or recognizing medicine consumption and/or container usage data and recording and storing same is adapted for transmitting information to a receiver and computer. The computer may be active or passive, i.e. do significant work with the data or simply convert it so it may be transmitted to and displayed on a remote display unit. Thus, for example, the device may be used to generate a signal which, after transmission and reception, may be amplified and then converted from analog to digital using a state of the art analog digital converter and then the signal would be used to perform compliance calculations on the computer. Additionally, frame 6 of Figure 1, step (C) involves the pre-programming of the device or the computer to store prescription requirements, to recognize various information such as indicated and to determine or calculate compliance requirements and to compare these to actual data. The system may involve storing sequential information e.g. dosage frequency data, so as to determine a required regimen and to compare actual usage against the required usage on a periodic basis or at random times, and to provide feedback. Having thus preprogrammed the device and/or the computer to perform these functions as well as optional functions described below, the system may now be used to practice the method of the present invention.

Referring again to Figure 1, frame 8 shows the first step (1) wherein data produced by an automatic compliance monitoring device from a medicine container is transmitted to said receiver and computer at least from time to time. As used herein, "from time to time" may be after each dosage is taken or at set intervals or at random intervals. Transmission could, alternatively, be continuous. Frame 10 shows the second step wherein the device or computer performs the functions preprogrammed per step (C), frame 6, discussed above. The computer recognizes the difference between the actual data and the dosage requirements of a patient after it calculates the required usage based on the dosage amount and frequency. Frame 12 shows the third step wherein a remote display unit receives the results of the compliance comparison, and frame 14 shows the fourth step wherein the computer displays compliance results for patient monitoring at a remote location.

As can be seen, the computer used in the present invention may be any conventional computer system and may be interlinked by way of modem or radio transmission or any other computer linking possibilities.

Figure 2 illustrates another diagrammatic representation of a present invention system. Here, like frames to Figure 1 are like numbered and are identically described. In this embodiment, however, as shown in frame 16, step (C) calls for providing an amplifier, second transmitter and second receiver. In frame 18, programming is as in frame 6 of Figure 1.

In the first step (1) shown in frame 20 of Figure 2, the data is transmitted, received, amplified and re-transmitted to a second receiver and then to one or more computers. Thus, a small, battery powered transmitter may transmit data to a remote but local receiver, which may then boost the data by amplifying same and re-transmitting to another receiver and then to one or more computers. Steps (2), (3), and (4) shown by frames 22, 24 and 26 of Figure 2 illustrate the same steps, (2), (3) and (4) as shown in Figure 1.

Referring now to Figure 3, there is shown a component 1 having an automatic compliance monitoring device, radio transmitter, power source and medicine container. The device provides data to the transmitter in radio transmission form and this is transmitted to receiver/computer 3 which is in turn connected to remote display unit 9. Additionally, receiver/computer 3 is connected to an optional, remote computer for professional or hospital use shown as 7 and when utilized this is connected to remote display unit 9. Optionally, inputs on other patient data may be fed into receiver/computer 3 and these optional inputs are shown as block 11. Also, optional patient display unit 5 may be connected to the system for automatic feedback and/or instructions from a professional who is monitoring the patient's medicine regimen. Further if a professional or hospital is monitoring patient's medicine regimen, then computer 7 and remote display unit 9 may be interconnected with a plurality of other patient inputs 13 and thus professionals may sequentially or randomly monitor a plurality of patients with the same system. This may be beneficial for convalescent homes, cancer treatment centers, rehabilitation centers and the like where patient progress and medicine regimen may be monitored from a single computer station, as well as to other data collection centers.

Figure 4 illustrates another schematic diagram of an alternative embodiment of the present invention. Most of the block frames shown are the same as those shown in Figure 3 and like parts are like numbered. However, in this embodiment, the transmitter from component 1 sends data to component 2 which includes a receiver, amplifier and re-transmitter. The re-transmitter forwards data by transmitting to component 3. For example, component 2 may be located in a home, in a hospital room, at a radio tower or close to or a significant distance from component 1 depending upon the power of the component 1 transmitter. Subsequent functions are similar to those described in conjunction with Figure 3 above.

An optional feature involves the use of satellite reception and re-transmission shown as component 4 in Figure 4. In other words, the transmitter on the medicine container may transmit to a booster transmitter which may then transmit to as many receiver re-transmitter set ups as desired, with appropriate amplification as needed.

In one preferred embodiment of the present invention, the medicine taker or user of the system may trigger an automatic transmission upon opening the container to input with the device and the computer each time the medicine is taken. Thus, in this embodiment, the expression relating to providing input from the device to transmit to the receiver and the computer "from time to time" refers to each time it is used. In this manner, optimum monitoring is achieved so that if there is an overdosage or a missed dosage, the present invention system will alert the user, or a professional or both of the deficiency or overdosage. Additionally, the system may, as mentioned, be used to provide monitoring for more than one medication at a time. This may be done by including an optional identifier whereby the compliance monitoring device for each medication has a code which is transmitted with the compliance data and read by and properly identified by the computer before the computer calculates and compares actual and required dosages. Alternatively, other ways of discerning advice for one medication from another may be included without exceeding the scope of the present invention.

In another preferred embodiment of the present invention, the system is used to also monitor heart rate, blood pressure, glucose, cholesterol, blood cell count, respiration, body weight or other physical characteristic or characteristics and these may be monitored by the patient or by a professional. Further, or in addition to the foregoing, the system may be used to also monitor compliance with a physical regimen such as a physical exercise program or a physical therapy program. This may be done by having a user active system wherein the user must feed in information to a transmitter for transmission to the receiver and the computer each time an exercise or a therapy session occurs or, more preferably, the system itself may be interlinked with actual exercise equipment such as treadmills, exercise bicycles, rowing machines; weight pulls, etc. and direct information from the exercise equipment will be communicated to the computer via one or more transmitters and receiver(s) and subsequently to the monitor to assure compliance by the patient.

In any of the above embodiments, the present invention in its more refined embodiment may include computer recognition and feedback of actual times and dates for every required dosage (specific day and/or time of day) and for every actual dosage removed from the medicine container. In other words, the system will provide the patient and/or professional with output showing actual versus required usage on a time based dosage comparison. When this mode is utilized, the computer will be provided with necessary information to generate requirements and the patient may input the computer with data from the compliance monitoring device of the medicine container at each use of the medicine container.

While the computer described above is generally preprogrammed to receive data from the automatic compliance monitoring device radio transmission and to process that data, the computer may be more complex or less complex without exceeding the scope of the present invention. For example the computer may be merely a unit that reads electronic information provided to it and converts it for transmission to a display unit. Alternatively, the computer may include any or all of the previously mentioned comparison and reporting functions and optional functions any may also include means for a patient to provide subjective information back to a hospital or doctor such as how the patient feels or how the patient is responding to the medication.

Obviously, numerous modifications and variations of the present invention are possible in light of the above teachings. It is therefore understood that within the scope of the appended claims, the invention may be practiced otherwise than as specifically described herein.

Claims

1. A method of monitoring a patient's medicine compliance which comprises:

   (a) providing an automatic compliance monitoring device, which device automatically tracks at least one type of patient medicine compliance data, said device being connected to a medicine container;

(b) providing a wave energy transmitter and a power source to drive said transmitter for transmission of said patient medicine compliance data to a remote location, said transmitter being electronically connected to said automatic compliance monitoring device for said transmission and said data transmitter and power source being connected to said medicine container;
(c) providing a receiver at said remote location and providing a computer to which said receiver inputs patient medicine compliance data;
(d) at least from time to time, transmitting patient medicine compliance data from said transmitter to said receiver and computer;
(e) having either said device or said computer programmed to store the prescribed medicine dosage and regimen of said container;
(f) having either said device or said computer programmed to calculate compliance requirements for each dosage administration for the prescription period of the medicine and for comparing the actual medicine consumption or container usage with the compliance requirements;
(g) connecting said computer to a display unit at a remote location away from the automatic compliance monitoring device; and,
(h) visually displaying the compliance results on said display unit to permit compliance monitoring.

2. The method of claim 1 wherein two computers are used, a first computer being located so as to be readily available to receive raw data from said automatic compliance monitoring device and a second being remotely located with said display unit.

3. The method of claim 2 wherein said first computer includes a display unit to provide corrective instructions to a patient when appropriate.

4. The method of claim 3 wherein said first computer is programmed to provide specific day and/or time of day information to display compliance information to a patient on its display unit.

5. The method of any of claims 1 to 4 wherein said transmission is to a professional for compliance monitoring.

6. The method of any of claims 1 to 5 wherein the method is repeated for a plurality of different containers of medicine with different automatic compliance monitoring devices and the computer determines and stores compliance information for each of said plurality of different devices.

7. The method of any of claims 1 to 6 wherein said automatic compliance monitoring device, said radio transmitter and said power source are located in a cap portion of a medicine container.

8. The method of claim 7 wherein said automatic compliance monitoring device is a cap removal counting device.

9. The method of claim 7 wherein said said automatic compliance monitoring device is a weighing device.

10. The method of and of claims 1 to 6 wherein said automatic compliance monitoring device, said radio transmitter and said power source are located in a base portion of a medicine container.

11. The method of claim 10 wherein said automatic compliance monitoring device includes an optical scale feature to measure medicine container content.

12. The method of any of claims to 1 to 11 wherein said receiver is located in a first remote area from said device and said computer is located at a second remote area from said device and said receiver and computer are connected to one another by additional wave energy transmission..

13. A system for patient medicine compliance and patient status monitoring, which comprises:
(a) a medicine container having a cap portion and a base portion;
(b) at least one automatic compliance monitoring device which automatically tracks at least one type of data related to actual medicine consumption or container usage, said device being connected to a medicine container;
(c) a wave energy transmitter and power source for transmission of patient medicine compliance data, said transmitter being electronically connected to said automatic compliance monitoring device and said transmitter and power source being connected to said medicine container;
(d) a receiver at a remote location from said radio transmitter;

(e) a computer connected to said receiver to receive input therefrom on patient medicine compliance data;
(f) a display unit connected to said computer to permit patient medicine compliance monitoring;

Further, wherein either said device or said computer is programmed to store prescribed medicine dosage and regimen of said container and having either said device or said computer programmed to calculate compliance requirements for each dosage administration for the prescription period and for comparing the actual medicine consumption or container usage with the complaince requirements to display comparison results on said remote display unit.

14. A patient medicine compliance system component, which comprises:
(a) a medicine container having a cap portion and a base portion;
(b) an automatic compliance monitoring device which atuoamtically tracks at least one type of patient medicine compliance data and being connected to said medicine container;
(c) a wave energy transmitter and power source to drive the transmitter for transmission of said patient medicine compliance data to a remote location, the transmitter being electronically connected to said automatic compliance monitoring device and the transmitter and power source being connected to said medicine container.

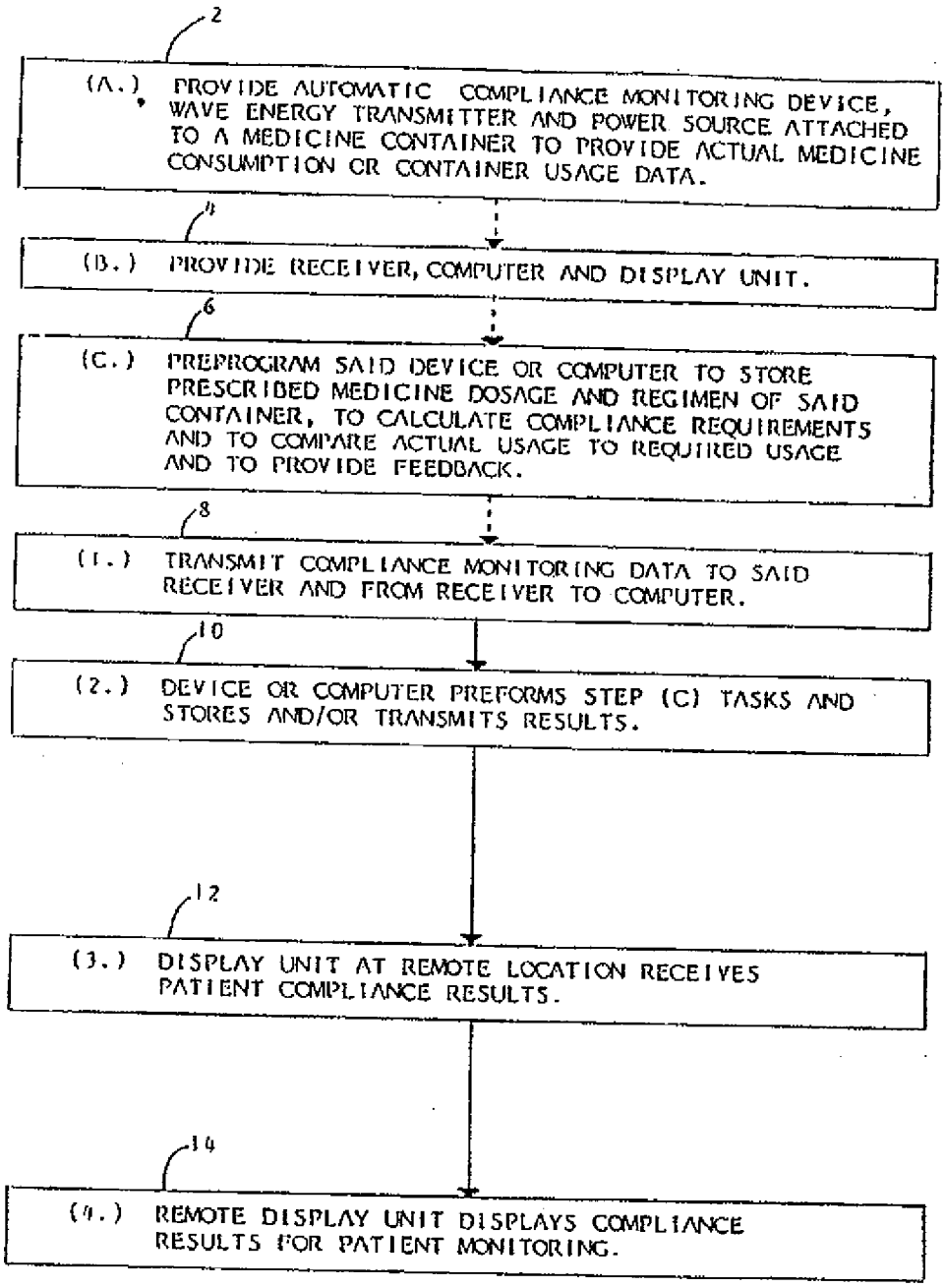

2
(A.) PROVIDE AUTOMATIC COMPLIANCE MONITORING DEVICE, WAVE ENERGY TRANSMITTER AND POWER SOURCE ATTACHED TO A MEDICINE CONTAINER TO PROVIDE ACTUAL MEDICINE CONSUMPTION OR CONTAINER USAGE DATA.
4
(B.) PROVIDE RECEIVER, COMPUTER AND DISPLAY UNIT.
6
(C.) PREPROGRAM SAID DEVICE OR COMPUTER TO STORE PRESCRIBED MEDICINE DOSAGE AND REGIMEN OF SAID CONTAINER, TO CALCULATE COMPLIANCE REQUIREMENTS AND TO COMPARE ACTUAL USAGE TO REQUIRED USAGE AND TO PROVIDE FEEDBACK.
8
(1.) TRANSMIT COMPLIANCE MONITORING DATA TO SAID RECEIVER AND FROM RECEIVER TO COMPUTER.
10
(2.) DEVICE OR COMPUTER PREFORMS STEP (C) TASKS AND STORES AND/OR TRANSMITS RESULTS.
12
(3.) DISPLAY UNIT AT REMOTE LOCATION RECEIVES PATIENT COMPLIANCE RESULTS.
14
(4.) REMOTE DISPLAY UNIT DISPLAYS COMPLIANCE RESULTS FOR PATIENT MONITORING.

FIG. 1

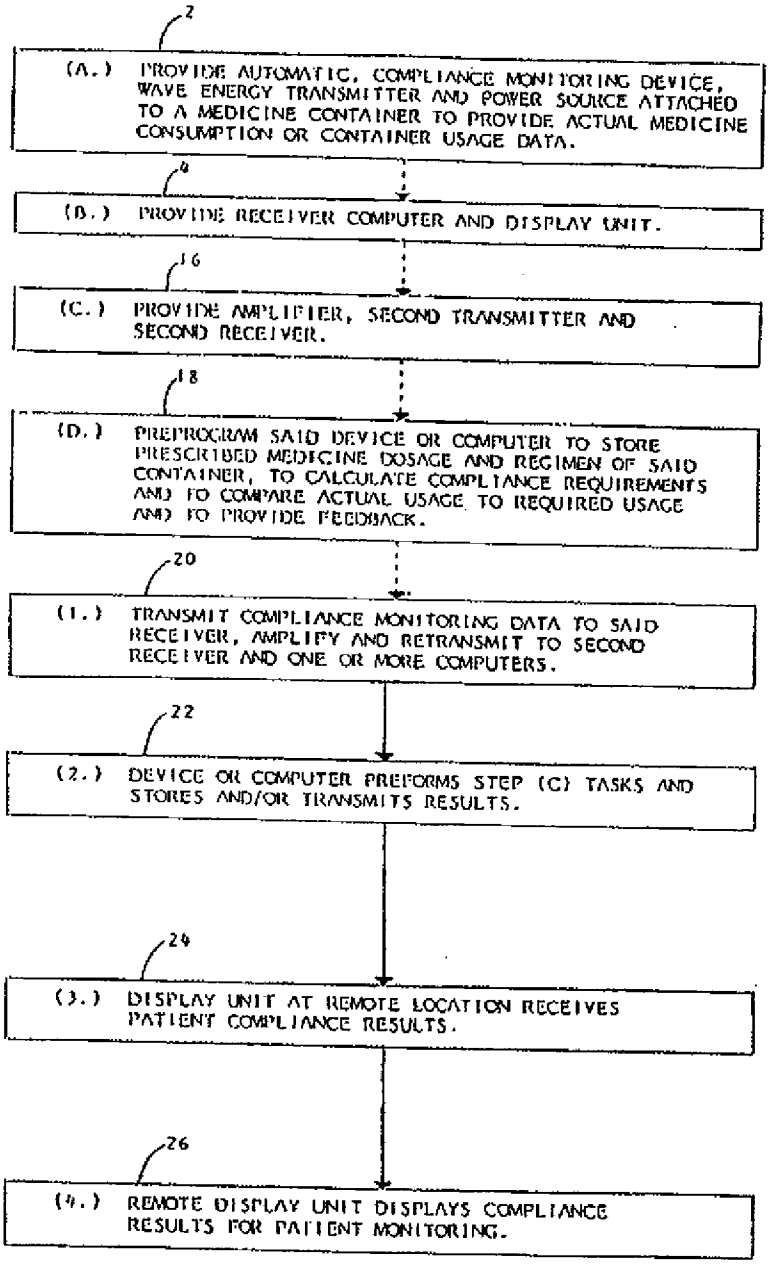

2
(A.) PROVIDE AUTOMATIC, COMPLIANCE MONITORING DEVICE, WAVE ENERGY TRANSMITTER AND POWER SOURCE ATTACHED TO A MEDICINE CONTAINER TO PROVIDE ACTUAL MEDICINE CONSUMPTION OR CONTAINER USAGE DATA.
4
(B.) PROVIDE RECEIVER COMPUTER AND DISPLAY UNIT.
16
(C.) PROVIDE AMPLIFIER, SECOND TRANSMITTER AND SECOND RECEIVER.
18
(D.) PREPROGRAM SAID DEVICE OR COMPUTER TO STORE PRESCRIBED MEDICINE DOSAGE AND REGIMEN OF SAID CONTAINER, TO CALCULATE COMPLIANCE REQUIREMENTS AND TO COMPARE ACTUAL USAGE TO REQUIRED USAGE AND TO PROVIDE FEEDBACK.
20
(1.) TRANSMIT COMPLIANCE MONITORING DATA TO SAID RECEIVER, AMPLIFY AND RETRANSMIT TO SECOND RECEIVER AND ONE OR MORE COMPUTERS.
22
(2.) DEVICE OR COMPUTER PREFORMS STEP (C) TASKS AND STORES AND/OR TRANSMITS RESULTS.
24
(3.) DISPLAY UNIT AT REMOTE LOCATION RECEIVES PATIENT COMPLIANCE RESULTS.
26
(4.) REMOTE DISPLAY UNIT DISPLAYS COMPLIANCE RESULTS FOR PATIENT MONITORING.

FIG. 2

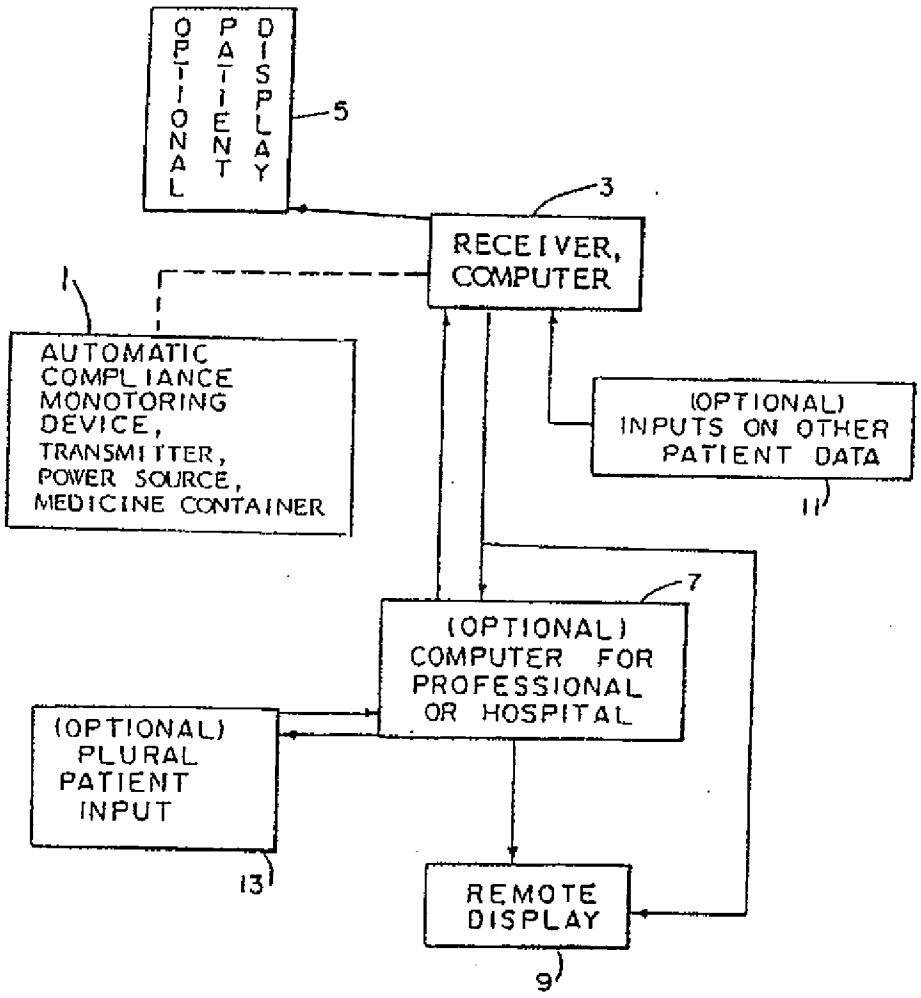

OPTIONAL PATIENT DISPLAY
5
3
RECEIVER, COMPUTER
1
AUTOMATIC COMPLIANCE MONOTORING DEVICE, TRANSMITTER, POWER SOURCE, MEDICINE CONTAINER
(OPTIONAL) INPUTS ON OTHER PATIENT DATA
11
7
(OPTIONAL) COMPUTER FOR PROFESSIONAL OR HOSPITAL
(OPTIONAL) PLURAL PATIENT INPUT
13
REMOTE DISPLAY
9

FIG. 3

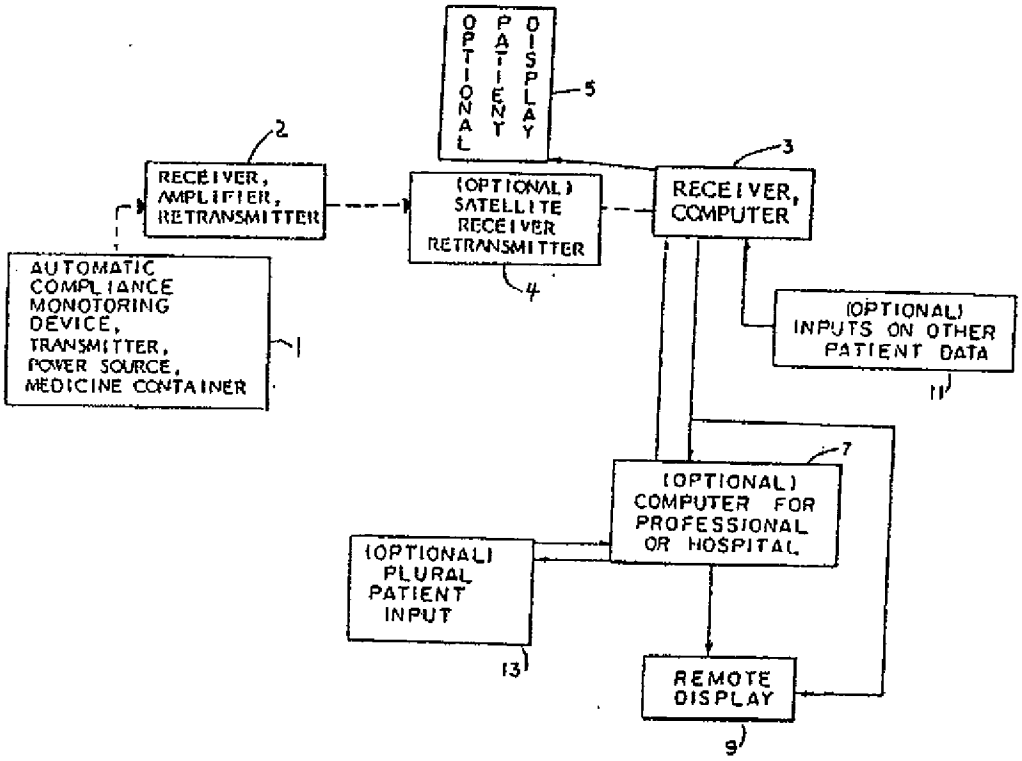

OPTIONAL PATIENT DISPLAY
5
2
RECEIVER, AMPLIFIER, RETRANSMITTER
(OPTIONAL) SATELLITE RECEIVER RETRANSMITTER
4
3
RECEIVER, COMPUTER
AUTOMATIC COMPLIANCE MONOTORING DEVICE, TRANSMITTER, POWER SOURCE, MEDICINE CONTAINER
1
(OPTIONAL) INPUTS ON OTHER PATIENT DATA
11
7
(OPTIONAL) COMPUTER FOR PROFESSIONAL OR HOSPITAL
(OPTIONAL) PLURAL PATIENT INPUT
13
REMOTE DISPLAY
9

FIG. 4

M

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-068051

(43)Date of publication of application : 14.03.1995

(51)Int.Cl. A63F 9/22
G04F 10/04

(21)Application number : 06-204521

(22)Date of filing : 05.08.1994

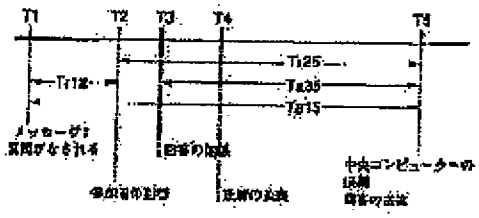
(71)Applicant : GEMPLUS CARD INTERNATL SA

(72)Inventor : PEYRET PATRICE

(30)Priority

Priority number : 93 9309679 Priority date : 05.08.1993 Priority country : FR

(54) SAFETY SYSTEM IN REMOTE PARTICIPATION IN INTERACTIVE GAME TO VERIFY EVENT IN TIME SERIES



(57)Abstract:

PURPOSE: To prevent an unfair practice by starting a count of continuous time intervals by a safely protected processor by a message of a transmitter, finishing it at connecting time to a central computer from a game machine for an answer, and verifying whether or not prescribed respective period lengths during this time can realize the prescribed relationship.

CONSTITUTION: A game machine counts a period length Tr12 regulated by time T1 to receive a message and time T2 when a TV viewer answers and a period length Ta25 regulated by the time T2 when the viwer answers and time T5 when an answer is sent to a transmitter/central computer. It also respectively counts a period length Ta35 between an answer time limit T3 and the time T5 and a period length Ta15 between the time T1 and the time T5. Whether or not a fuction of a value of an allowable range (Tr25>Ta35, and Tr12+Tr25=Ta15±) is realized during these counted period lengths (Tr25, Ta35, Tr12 and Ta15), is verified, and when it is not realized, an answer is rejected.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] Had the transmitter/central computer which transmits the code message received by the television set while a TV program is going on. It is a safety system in the remote participation to an interactive game. A TV viewer Read the broadcast message, have the possible game machine of returning the reply to the question made in these messages, and it sets to this system. It has a means by which a game machine counts a continuous period. Among these, the first period (Tr12) The message transmitted by the transmitter/central computer begins. The last period (Tr25) The connection with a transmitter/central computer from a game machine is completed. The first period It is prescribed by the time amount (t1) by which a message is received, and the time amount (t2) which a TV viewer answers. The last period (Tr25) It is prescribed by the time amount (t2) which a TV viewer answers, and the time amount (t5) by which a reply is sent to a transmitter/central computer. Further a game machine It has a means for transmitting a reply to a transmitter/central computer with the above-mentioned count result. The period when a transmitter/central computer is specified by the time amount (t5) to which the term (t3) of a reply and the reply were sent (ta35), A means to count the period (ta15) specified by the time amount (t1) to which the message was transmitted, and the time amount (t5) to which the reply has been sent, Tr25>Ta35 And relation called the value of Tr12+Tr25=Ta15** tolerance is checked. The safety system in the remote participation to an interactive game characterized by having the count and the check means which are constituted so that a reply may be refused, when this relation furthermore is not verified.

[Claim 2] The safety system in the remote participation to the interactive game according to claim 1 characterized by the count means of a game machine being constituted by the secured microprocessor which performs a clock pulse count program, and which is controlled by the clock.

[Claim 3] The safety system in the remote participation to the interactive game according to claim 1 characterized by constituting the count means of a game machine by count means controlled by the internal clock to perform a clock pulse count program.

[Claim 4] By the means for receiving the digital information which is a machine for participating in a program and attesting participation in cooperation with a remote central computer, and is sent from a central computer, and the participant The interface means for introducing the data element showing a participant's participation, The means for connecting with a central computer, a microprocessor and at least one secured electronic component equipped with the storage means, and at least one clock signal generating circuit are offered. The above-mentioned machine by time amount T1 If the digital message which has a predetermined gestalt is received, the microprocessor secured after delivery and verification by the microprocessor which had that message secured will record this message on that memory. The count of the time amount unit proportional to the period of the clock signal given by the clock signal generating circuit is started. By time amount T2 If a machine receives the data element about his participation from the TV viewer who owns this machine A machine transmits the data element to the secured microprocessor. With a means by which this microprocessor records that data into that memory with a required gestalt, records this instantaneous time amount counted value further, and connects with time amount T5, until the above-mentioned machine is connected with a central computer Shortly after the secured microprocessor continues a count and connection is made A microprocessor transmits the data element and counted value Tr12 and Tr25 about the memorized participation. The machine for participating in a program with which a central computer is characterized by refusing a reply in verifying that these values are in agreement with the counted value of itself and not being further in agreement.

[Claim 5] The machine for participating in the program according to claim 4 characterized by having had the chip card reading means and the chip card, and equipping the above-mentioned chip card with the component with which the gestalt of the integrated-circuit chip card which has a microprocessor, activity memory, and program memory was secured.

[Claim 6] It is central computer equipment which manages the participation to the broadcast scenario of the TV viewer who has an electronic participating machine. A time amount count means, A means to broadcast a digital message to each electronic participating machine, and the means for making connection with each electronic participating machine, If it has the storage processing means and a new broadcast scenario is started To time amount T1, this central computer equipment uses a suitable transmission channel, and broadcasts a digital message at each electronic participating machine of a TV viewer. Furthermore, initialize a time amount count means, operate it, and a TV viewer memorizes time amount counted value to predetermined time amount T3 chosen as time amount it becomes impossible to participate in a scenario more than it. this -- a count -- continuing -- an electron -- participation -- a machine -- a central computer -- connecting -- having -- time amount -- ****** -- choosing -- having had -- time amount -- T -- five -- an electron -- participation -- a machine -- obtaining -- having had -- time amount -- counted value -- memorizing -- the following -- relation -- checking -- : -- Tr -- 25 -- > -- Ta -- 35 -- Tr25 is a count period by the electronic participating machine between T2 and T5 here. a Tr12+Tr25=Ta15** tolerance value -- Tr12 is equipment which is a count period by the electronic participating machine between T1 and T2, and Tr35 is a count period by T3 and the central computer between T5, and is characterized by Tr15 being a count period by the central computer between T1 and T5.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the unjust prevention system or safety system in remoteness or long-distance participation to an interactive game which verifies the time series of an event.

[0002]

[Description of the Prior Art] To enable participation to a viewer's game which is called for so that a viewer may answer for example, during broadcast to the question broadcast with [station] the advent of the so-called interactive television systems is desired. In order for a TV viewer to answer in the midst of such a game after the correct answer of a game is shown from an office, or to prevent a various-subjects lexicon and answering after referring to the reference database of arbitration in addition to this, the maximum reply time amount must be set up. Furthermore, in order that the feeders (a cable operator, broadcast studio, etc.) of service may avoid "being saturated" by the reply of thousands sent to coincidence, as for a reply of a TV viewer, it is desirable to make it not sent immediately. For that purpose, an are recording transmitting system is indispensable. In this system, it is a safe approach, and a reply of a TV viewer is memorized by the devices for the public (for example, a cable decoder, the game machine of dedication, etc.), and behind, it is that viewer's home and it is sent [it shifts time amount suitably and] by the suitable telecommunication means of a radiotelephone and other arbitration [a cable and].

[0003] There are some which were developed for example, developed by the interactive game networks (Interactive Game Networks) company as an example of such a system in the United States of America. In this system, a TV viewer has the small game machine with which a radio interface, the keyboard, the screen, the modem, and the security module were prepared. In order to understand actuation of such a system, please refer to drawing 1 which showed the time series of an event.

[0004] By time amount T1, a question is broadcast from the transmitter/central computer called a "central computer" below. These questions are broadcast with radio to the above-mentioned game machine. For example, at the time of initiation of a game of football, a TV viewer is called for so that the score of the first half may be expected. This question appears on the screen of a game machine. A reply is inputted through the key boat of a game machine by each TV viewer who has participated in time amount T2, and it is recorded on the insurance chip (thing of the type currently used by the smart card) with which the game

machine is equipped. A new broadcast signal locks all game machines in time amount T3, and it is made not to receive any replies any more to it after [of since a question is performed] several minutes. Then, the answer to a question is broadcast by time amount T four (in this example, T four is actually equivalent to halftime). Then, the reply recorded on time amount T5 is sent to the central computer of a game through an exchange type telephone network by the modem, and serves as certification of participation. If a TV viewer answers correctly, he/she will receive a certain prize thru/or prize.

[0005] American ****** According to a practice like [of No. 4,592,546] a publication, the date (time amount) of each event is recorded using the clock circuit which has sufficient precision installed in the game machine. When a reply of a participant is sent to the central computer of a game, the time amount recorded with the game machine is also sent to a central computer, and it is compared with the conventional time saved in it by the computer.

[0006] According to the practice otherwise proposed, in each public mold game machine, the reference clock signal transmitted from the central computer of a game and the electronic real time clock circuit synchronized for every fixed spacing (for example, wireless association) possess. The time amount T1 it is broadcast that a question is, and the time amount T2 by which a reply is made are recorded on a game machine (for example, recorded in the chip for smart cards by the secured approach). If connection is made to a game central computer, the time amount recorded as the reply will be spent as certification of participation. A central computer is within the limits which can permit the information concerning air time T1, and checks that T2 is a front [T3 / which is a reply term].

[0007]

[Problem(s) to be Solved by the Invention] In addition to this in the above-mentioned system, the user who had malice in the similar embodiment may record the control signals (a question, a locking instruction, clock synchronization signal, etc.) sent to his game machine on a suitable machine.

[0008] In that case, if the answer to a question is broadcast from an office or a special search or the place which he gets to know with the means of arbitration in addition to this comes when slightly behind, the individual with this malice can repeat a control signal in his own game machine, and can pretend the reply of real time. This becomes possible for the time amount of die length appropriate always enough passing before attainment of the reply to the central computer which a witness does not break into the individual who performs a fraud action in the privacy of a house, but is further expected from a degree from play termination. It is economically impossible to equip a game machine with the means for getting to know whether it is what slight delay is given, after a game machine is generated truly at the real time or the signal (this should be made by insurance) which it received from the outside is recorded completely without correction in them on it after all.

[0009] the France patent application 89th -- it applies as No. 06848 -- having -- the France patent application public presentation official report 2nd -- the patent exhibited as 647 619 No. -- and -- coming out -- the France patent application public presentation ****** the France addition patent 90th exhibited as 2 658 357 No. -- delaying a play to No. 01512 -- the system which enables unjust prevention is indicated. Time amount (or reply term) T3 it was broadcast for the central computer in the system that an answer was, The reply by the TV viewer counts the absolute time which passes between the time amount T5 sent to the central computer, and it sets to time amount T2. By reply of a TV viewer, local time count actuation within a game machine is started. To the time amount T5 by which information is sent to a central computer, it checks that this central computer is size more nearly rightly than absolute time T5-T3 which itself calculated [time amount T5-T2 measured with the game machine of********].

[0010] The timing chart shown in drawing 2 shows the above sequence. The approach proposed by this patent is not trustworthy by any means to a regrettable thing. A user is because it can show between a reply and connection with a central computer as if time amount T5-T2 [longer than the time amount which actually passed] passed by advancing a local time counter. This becomes possible only by correcting temporarily the oscillation frequency of the electronic clock circuit placed into the game machine.

[0011] The counter in a game machine is actually accessible for a user, unless it is protected physically (i.e., unless it is embedded in resin). Even if this circuit is supplied by any of an RC oscillator, a ceramic resonator mold oscillator, or a crystal oscillator, that original frequency can be distorted by few [an oscillating component] mismatches. Therefore, it is possible to make an oscillation frequency high by few percentages,

or to make it late, without being accompanied by exceptional difficulty. By making high the oscillation frequency of the oscillator supplied to the clock circuit of a game machine, the oscillation frequency of the oscillator of a game machine is made high waiting (it is waiting about an answer being broadcast live), and after that, and they can regain delay until term T3 passes over those who are going to perform a fraud action. Therefore, when this individual's game machine receives an inquiry from a central computer by time amount T5, time amount T5-T2 of the appearance given to this central computer become long actually more rather.

[0012] The method of equipping the microprocessor of a microcircuit card of a certain kind with the clock frequency detector for detecting the abnormalities of a clock frequency is learned. In order for the individual who is going to perform for example, a fraud action to prevent trying the "step-by-step" method to the program performed by the processor, this kind of detector operates, when the clock frequency supplied to this component is extremely low. such [typically] a low frequency detector -- the nominal frequency of the component -- 1MHz - 5MHz it is -- sometimes, it operates by less than about 500kHz. Serious lack of the precision in this kind of detector and the fact of existing only in order that it may detect an extremely low frequency mean that it cannot use it in order to prevent injustice above type.

[0013] This invention aims at conquering the fault of the system by which current use is carried out. The system set as the object of this invention can actually be used, in order that a TV viewer may verify certainly rightly the fact of having replied to the question between the terms determined by the transmitting person of time amount and a game to whom the question was given.

[0014]

[Means for Solving the Problem] The message secured using the code in which the first spacing is transmitted by the transmitter begins [the system proposed here counting the time interval which continues by the secured processor (for example, microcircuit card processor)], and the last spacing is ended by making connection with a central computer from a game machine, in order to send the certification of a reply to a central computer.

[0015] More, a detail will be provided with the safety system equipped with the transmitter/central computer which transmits the code message received by the television set during advance of a TV program in the remote participation to an interactive game, if based on this invention. A TV viewer reads the broadcast message and it has the possible game machine of returning the reply to the question made in these messages. The die length Tr12 of the period when a game machine is specified in this system by the time amount t1 by which a message is received, and the time amount t2 which a TV viewer answers, It has a means to count the die length Tr25 of the period specified by the time amount t2 which a TV viewer answers, and the time amount t5 by which a reply is sent to a transmitter/central computer, and is [0016]. The die length ta35 of the period when a transmitter/central computer is specified by the time amount t5 to which the term t3 of a reply and the reply were sent, It has a means to count the die length ta15 of the period specified by the time amount t1 to which the message was transmitted, and the time amount t5 to which the reply has been sent. Furthermore, relation called the value of Tr25>Ta35 and Tr12+Tr25=Ta15** tolerance was checked, and when this relation is not verified further, it has a count means to refuse a reply. The count means of a game machine is constituted by the secured microprocessor which performs a clock pulse count program and which was controlled by the clock.

[0017] The machine for according to this invention, participating in a program and attesting participation in cooperation with a remote central computer further By means to receive the digital information sent from a central computer, and the participant The interface for introducing the data element showing a participant's participation, It has the means for connecting with a central computer, a microprocessor and at least one secured electronic component equipped with the storage means, and at least one clock signal generating circuit, and is [0018]. If a machine receives the digital message which has a gestalt predetermined by time amount T1 The microprocessor secured after delivery and verification by the microprocessor which had that message secured records this message on that memory. The count of the time amount unit proportional to the period of the clock signal given by the clock signal generating circuit is started. By time amount T2 When a machine receives the data element about his participation from the TV viewer who owns this machine, a machine That data element is transmitted to the secured microprocessor, this microprocessor records that data into that memory with a required gestalt, and records this instantaneous time amount counted value

further, and it is [0019]. Shortly after the secured microprocessor continues a count and connection is made by time amount T5 until the machine is connected with a central computer by the means which connects, a microprocessor transmits the data element and counted value Tr12 and Tr25 about the memorized participation, a central computer verifies that these values are in agreement with the counted value of itself, and a reply can be refused when not further in agreement.

[0020] Furthermore, the central computer equipment which manages the participation to the broadcast scenario of the TV viewer who has an electronic participating machine according to this invention is equipped with the time amount count means, a means to broadcast a digital message to each electronic participating machine, the means for making connection with each electronic participating machine, and the storage processing means, and is [0021]. If a broadcast scenario is started, to time amount T1, this central computer equipment will use a suitable transmission channel, and will broadcast a digital message at each electronic participating machine of a TV viewer. And initialize a time amount count means, operate it and an audience memorizes time amount counted value to predetermined time amount T3 chosen as time amount it becomes impossible to participate in a scenario more than it. : which continues this count, memorizes the time amount counted value obtained by the electronic participating machine to the time amount T5 chosen as time amount by which an electronic participating machine is connected to a central computer, and checks the following relation [0022] Tr25>Ta35 and a Tr12+Tr25=Ta15** tolerance value -- Tr12 is a count period by the electronic participating machine between T1 and T2, :Tr25 is a count period by the electronic participating machine between T2 and T5 here, and Tr15 is [Tr35 is a count period by T3 and the central computer between T5, and] a count period by the central computer between T1 and T5.

[0023] Each game machine (electronic participating machine) is equipped with the microprocessor from which it secured for microcircuit cards. According to another example, this microcircuit may be contained in the card which has a gestalt like the card of a bank inserted in the machine which functions as a card reader of an available class commercially. Or in addition to this, the secured circuit may be built in portable goods other than a card, for example, the key of plastics, and the goods of arbitration considered to be suitable.

[0024] The secured circuit can also be directly installed to the main circuit component of a machine, as it demounted, and it mentioned above further, when it was thought that it is not necessary to suppose that it is possible. Please understand the word "secured microprocessor" to be what shows the microprocessor to which the protection of arbitration used for use of a smart card like the banking card which for example, the current bank has distributed is applied. By the following publications performed with reference to attached drawing, the advantage of others of this invention will become clear. The following publications are the things for instantiation only, and do not limit this invention.

[0025]

[Example] Drawing of drawing 4 shows the secured system in the participation to a game which enables measurement actuation of the sequence stated to the following shown in Table 1 of the tail of this specification. This system has a transmitter / central computer 1 equipped with the central computer unit 20 which it is combined with the TV program transmitter 10 and its transmitter 10, for example, can transmit a game message to the above-mentioned patent application with an enciphered gestalt like a publication.

[0026] The transmitter/central computer is connected to the receiver arranged at user ** through the transmission means 30. The user who expects participation of the game broadcast reads the coded message receiving on a plane, and owns the game machines L1-Ln connectable with the central computer in a standard approach. Time amount [the time amount T1 to which a message is transmitted], i.e., when a TV viewer is asked, a transmitting center and the game central computer 1 send the message of a code which signed game machines L1-Ln, for example by the well-known secret key for card actuation.

[0027] The transmission channel 30 which is a DCH of the dedication prepared in the channel (a channel of FM radio like [For example,] U.S.'s interactive game networks) of the inside of the same channel as the signal broadcast (for example, inside of a return frame), the channel (for example, HF channel of dedication on the cable which transmits two or more television channels) which it became independent of in the same medium, or a different medium can perform dispatch of this message.

[0028] A DCH does not need to be the thing of the one direction nature from the transmitter and service provider of a signal to a TV viewer. A game machine L1 will be sent to the secured component CS which demounted this so that it might explain to the following in a game machine, and was installed in the possible

medium, if this signal that appears on the screen 41 of a television set 40 in the form of a code is received. A game machine can equip the above-mentioned patent with the well-known type electronic-circuitry component like a publication, and a game machine can send a reply message to a central computer in response to the message which appears in the screen of television by it.

[0029] It is shown in drawing 5 and the secured component CS is volatility and nonvolatile memory 110, i.e., RAM activity memory, and the ROM program memory 120. And EEPROM data memory 130 Microprocessor 100 which it had It has. Component CS -- clock signal generator 150 of a game machine from -- a clock pulse -- winning popularity -- further -- block 140 It has a connecting means to the game machine which expressed. It is a microprocessor 100 when a message appears on a screen. That truth is verified by the usual approach and the activation of a time amount count subprogram based on a clock pulse is made to start in response to this message. This subprogram is contained in the ROM memory 120.

[0030] Clock frequency 150 by which the secured microprocessor is actually supplied to the microprocessor instead of absolute time A proportional time amount unit is counted. It is because a microprocessor does not have time criteria other than this clock signal at all. Furthermore, secured microprocessor 100 That nonvolatile memory EEPROM130 The code message (or shadow of this message) which made count actuation start is recorded.

[0031] In order to understand the following things more clearly, please refer to Table 1 of the tail of this specification. Microprocessor 100 from which this reply was secured when the TV viewer replied to the question by time amount T2 using his game machine L1 It is sent and is a microprocessor 100. It is the well-known volatile memory 130 about it. It records and the time amount counted value which had reached further when the reply of a user was received is recorded. Microprocessor 100 secured just behind this event A count is continued. It does not change T3 that it is the absolute term which a TV viewer can answer to a question. Nothing happens to this time amount specially at a game machine. That is, information is not received but the secured microprocessor continues the count of time amount.

[0032] The central computer itself equipped with the standard processing means 20 containing the central-process unit 21 and memory 22 (the count program is loaded to one of them) by time amount T3 starts time amount count actuation. A central computer is a core, and since it is used as criteria, it calls this count a count "absolutely" below. The count adopted shall be very stable and shall express the approximation near the real time as much as possible. T four is absolute time amount by which the answer to a question is given on a TV viewer's screen. Nothing special happens to this time amount.

[0033] A transfer of the specific data element of each TV viewer who participated in the game is performed by connecting game machines 40-40n to a central computer 1 after time amount T four (for example, several hours after a game). Since many TV viewers may have participated, probably connection is programmed to be carried out at night. The thing and direction which were used for a TV viewer's game machine broadcasting the DCH described previously are connected to a central computer through opposite "return channel." This return channel may be directly formed on a distribution cable, if television is broadcast by the bidirectional cable. A return channel can also be set up on the switched telephone network with an easy modem. In addition, use of a possible return channel can be considered. The reference number 30 in drawing 4 expresses one or more possible transmission channels of being equipped.

[0034] Microprocessor 100 subsequently secured when connection was made by one of the above-mentioned means between the central computer 1 and a TV viewer's game machine L1 (Ln) A standard justification certification activity is started, the justification of a central computer is proved, and the justification of itself is proved with a central computer. The device of this justification certification shall be based on the code system using a secret key or a well-known public key, without completely changing the purpose of this invention. Microprocessor 100 secured during connection The value of the reply which was given to the central computer by the TV viewer and recorded on it by time amount T2 is sent.

[0035] At this invention, it is a microprocessor 100. The value of Tr12 and Tr25 is further sent to a central computer. Here, Tr12 is the relative local time calculated in a TV viewer's game machine by the microprocessor secured between T1 and T2 (it is shown in drawing 3 like). Tr25 is the relative local time calculated by the secured same microprocessor between T (as [show / in drawing 3])2, and T5. It is transmitted with the checksum which used the code and the value of the time amount which the reply of a TV viewer and the game machine L1 calculated on that spot can also be enciphered by well-known arbitrary

encryption algorithms from the reasons of secrecy depending on the case, in order to guarantee the integrity. This does not influence the principle of this invention at all.

[0036] Here, time amount is shown "absolutely" and Ta15 considers as the thing which was calculated by the central computer between T (as [show / in drawing 3])1, and T5, by which Ta35 was calculated with the central computer among T5 with T3 (as [show / in drawing 3]) and which shows time amount "absolutely." If based on this invention, a central computer will check that it is Tr25>Ta35 first in that case, and it will check that it is a Tr12+Tr25=Ta15** tolerance value (the tolerance value is set up beforehand). A reply will be accepted if these relation is verified. When that is not right, a central computer refuses this.

[0037] That is, it is the clock 150 given to a card between T2 and T5 in order for him to make the value of Tr25 increase artificially, if the individual who is going to perform a fraud action is going to show as it answered before T3 although he answered in practice after T3. A frequency must be raised. However, since the sum total of Tr12+Tr25 stops becoming equal to a Ta15** tolerance value, this actuation will be revealed.

[0038] Although activation is difficult, the still possible only malfeasance lowers only a part equal to the amount and accuracy which must raise the frequency of the clock signal between T2 and T5, in order that the sum total of Tr12+Tr25 may maintain the legal value for the frequency of the clock signal given to the microprocessor secured between T1 and T2. In order to make this impossible, time amount T3 should just check that it is adjustable to time amount T1 (that is, what is necessary is just to make it, in order to reply to a question (the time amount which a viewer is allowed differ for every question)). Therefore, since the individual who is going to perform a fraud action does not understand the value which must raise the frequency of the clock signal between T2 and T5 continuously, he cannot foreknow the value which can lower the frequency of a clock signal between T1 and T2.

[0039] It is also possible to guarantee events T1 and T2, T3, and the exact time series of T5 by the secured microprocessor which is used by the approach standard as an object for smart cards by this invention, and does not have the exact reference clock signal with which especially itself is secured by it.

[0040] The component which drawing 6 shows the specific example in this invention, and was secured takes the gestalt of the integrated circuit chip of a memory card C. That is, in order that this machine may read the message displayed on the screen and may input a TV viewer's response, it has the part L1 used for connection with a central computer, and the memory card which demounted and was equipped with the possible part, i.e., a microprocessor. For this reason, a part L1 is suited with the slot F for L1 to receive a card and the connector C of a card, and there is a connector which enables L1 to function as a memory card reader (not shown) in it. If it carries out with this example, especially this invention is applicable to the subscriber television systems which have already used the smart card, in order to secure the security to scramble discharge of a television signal.

[0041]

[Table 1]

トランスミッタ／ ゲーム中央コンピュータ	ゲーム機械／受信機	テレビ視聴者／ 参加者
ゲームメッセージ →	メッセージ受信 （時間Ｔ１） クロックパルスのカウント、 メッセージの記憶	
	回答の受信および記憶 ←	回答
	カウント値の記憶	（時間Ｔ２）
回答期限（Ｔ３）		
正解 →	正解の受信	
計算 ←	中央コンピュータとの	
Ｔａ１５とＴａ３５	接続設定	
回答の受信および	記憶されていた回答の送信	
Ｔｒ１２とＴｒ２５	Ｔｒ１２とＴｒ２５の送信	
チェック Ｔｒ２５＞Ｔａ３５ Ｔｒ１２＋Ｔｒ２５＝ Ｔａ１５±許容範囲値		

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the timing chart showing the time series of the event of a game.

[Drawing 2] It is the same timing chart as drawing 1 showing the count sequence by the Prior art.

[Drawing 3] It is the same timing chart as drawing 1 showing the count sequence of this invention.

[Drawing 4] It is drawing having shown the principle of a game system.

[Drawing 5] It is detailed drawing of a safety system by this invention.

[Drawing 6] It is drawing of the machine in a specific example.

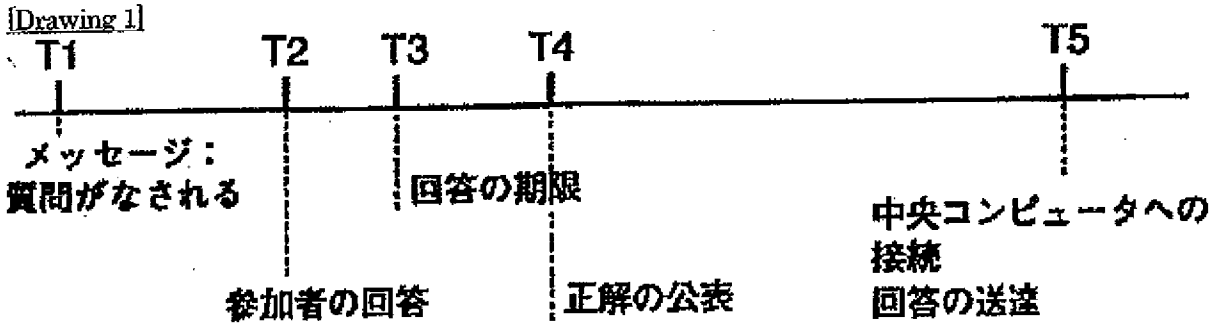
[Description of Notations]

1 ... Game central computer

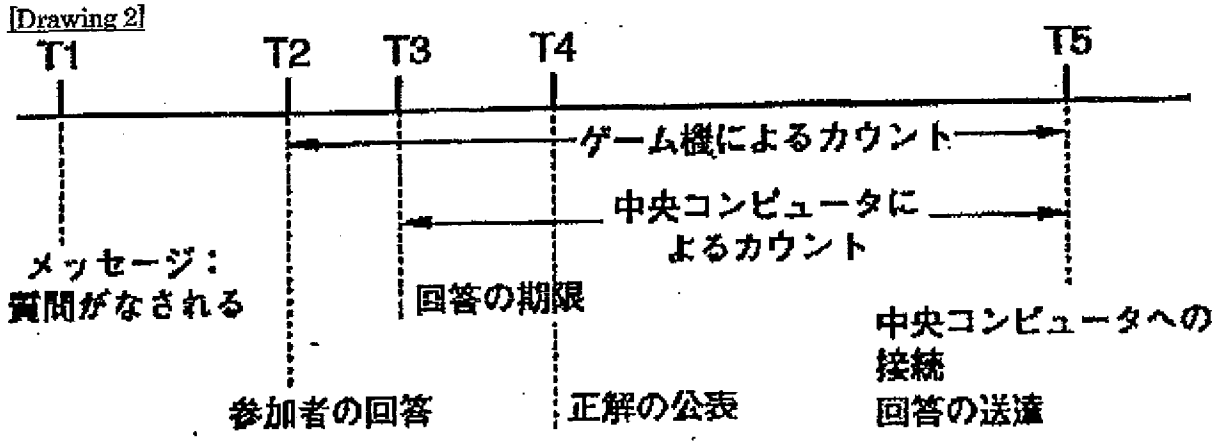
10 ... Transmitter
20 ... Central computer unit
21 CPU ... Central-process unit
22 ... Memory
30 ... Transmission channel
40 or 40n ... Television set
41 ... Screen
100 ... Microprocessor
110 ... RAM Activity Memory
120 ... ROM Program Memory
130 ... EEPROM Data Memory
140 ... Connecting Means
150 ... Clock Signal Generator
CS ... Secured component
C ... Memory card
F ... Slot
L1, Ln ... Game machine

DRAWINGS

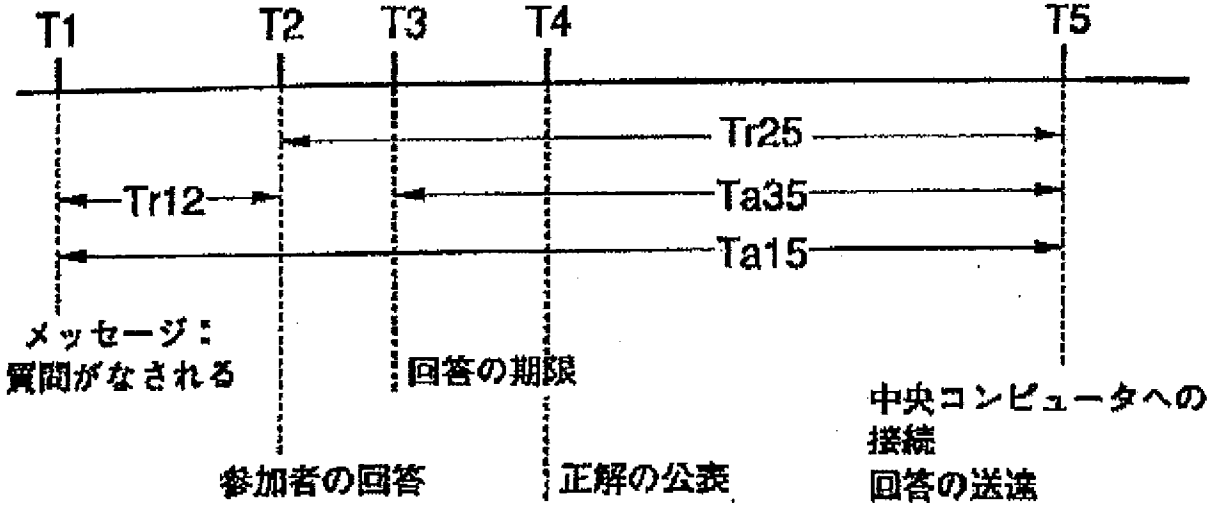
[Drawing 1]



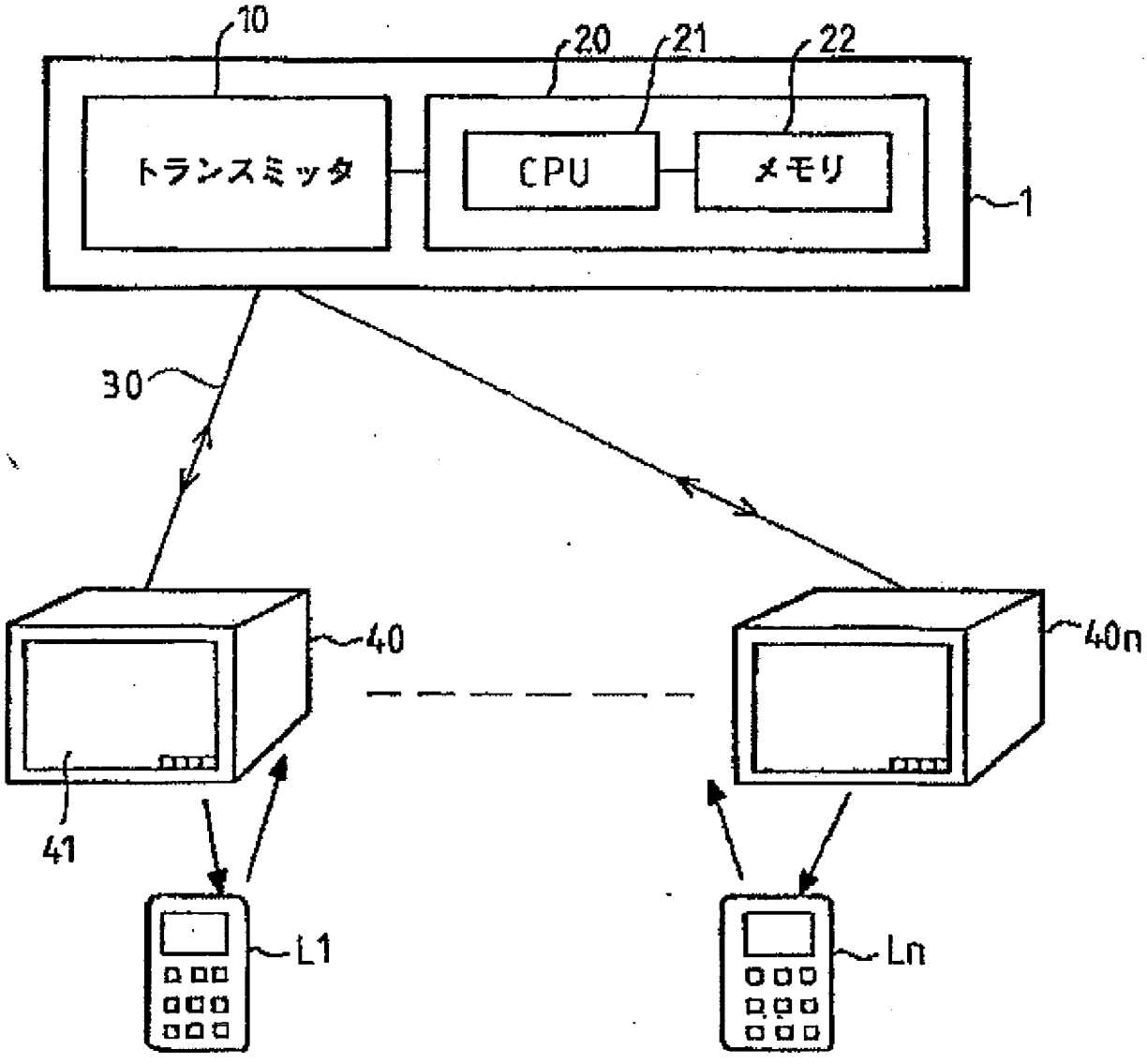
[Drawing 2]



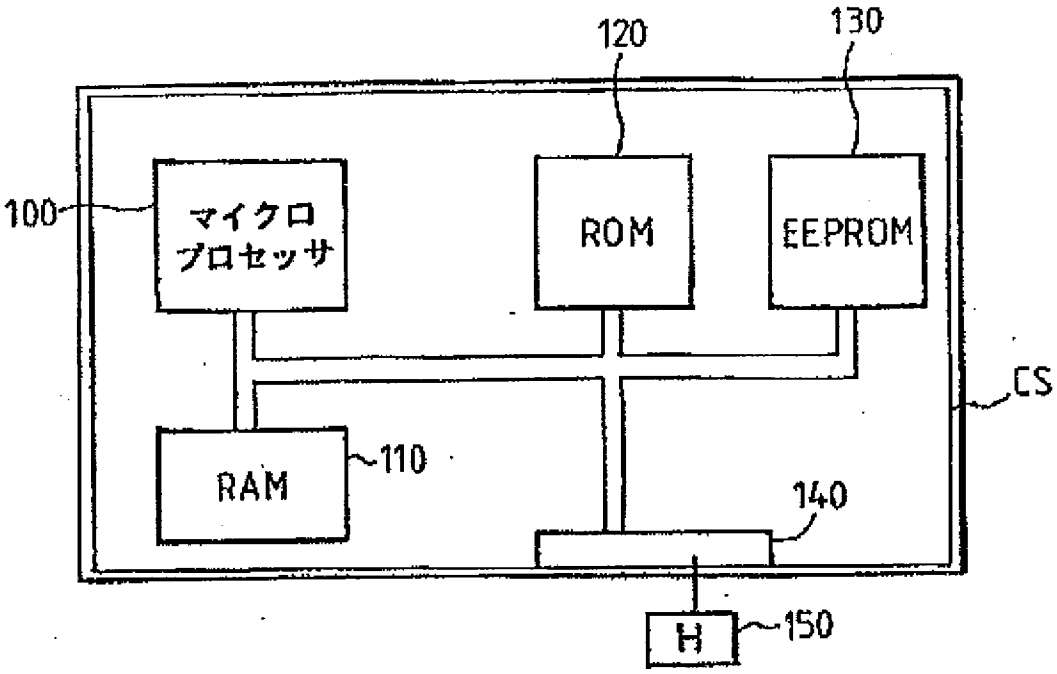
[Drawing 3]



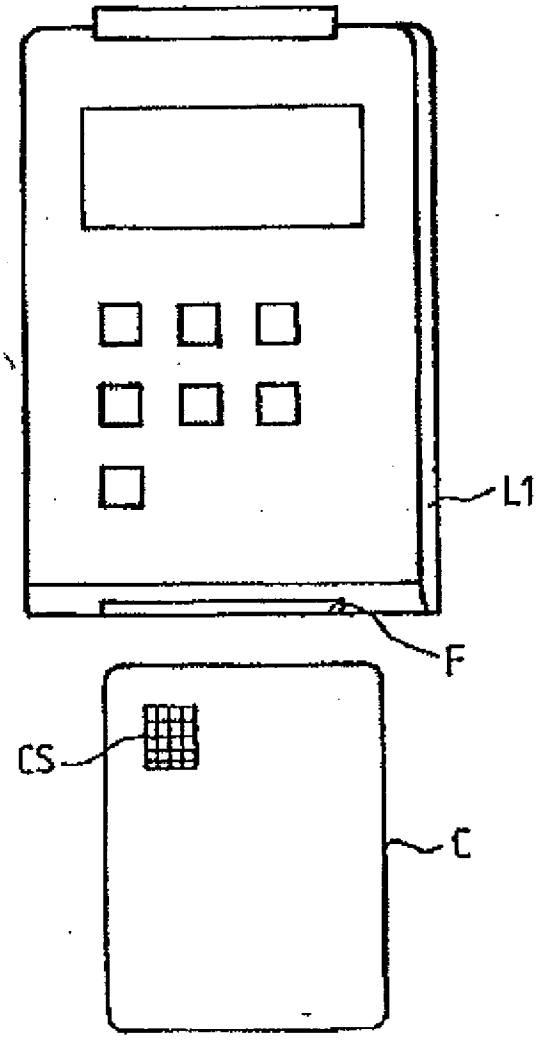
[Drawing 4]



[Drawing 5]



[Drawing 6]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－68051

(43)公開日　平成7年(1995)3月14日

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ａ６３Ｆ　9/22	Ｇ			
	Ｈ			
Ｇ０４Ｆ　10/04		9008－2F		

審査請求　未請求　請求項の数6　ＦＤ　（全９頁）

(21)出願番号　特願平6－204521

(22)出願日　平成6年(1994)8月5日

(31)優先権主張番号　９３０９６７９

(32)優先日　1993年8月5日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　591032013
ジェムプリュス　カード　アンテルナショナル　ソシエテ　アノニム
GEMPLUS CARD INTERNATIONAL SOCIETE ANONYME
フランス国　13420　ジェムノ　パルク　ダクティヴィテ　ドゥ　ラ　プレーヌ　ドゥ　ジュク　アヴニュ　ドュ　ピック　ドゥベルターニュ（番地なし）

(72)発明者　パトリス　ペイレ
フランス国　シュマン　ドゥ　サン　フランソワ　ルクロ　ドュ　ポン（番地なし）

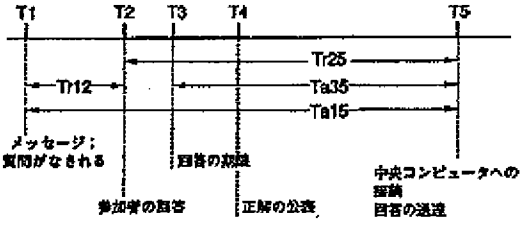
(74)代理人　弁理士　越場　隆

(54)【発明の名称】　イベントの時系列の検証を行う、対話式ゲームへの遠隔参加における安全システム

(57)【要約】

【構成】　安全保護されたマイクロプロセッサ（例えばマイクロ回路カード）を用いた連続する期間のカウントによって、イベントの時系列の検証を行う、対話式ゲームへの遠隔参加における安全システム。そのうち最初の期間（Ｔｒ１２）は、トランスミッタによって送信される暗号を用いて安全保護されたメッセージによって開始され、最後の期間（Ｔｒ２５）は、回答をトランスミッタの中央コンピュータに送るための、ゲーム機からトランスミッタの中央コンピュータへの接続によって終了される。

【作用】　テレビ放映される対話式ゲームに利用される。



(19)日本国特許庁（JP）　(12)公開特許公報（A）　(11)特許出願公開番号
特開平7－255950
(43)公開日　平成7年(1995)10月9日

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI	技術表示箇所
A63F 9/22	G M			

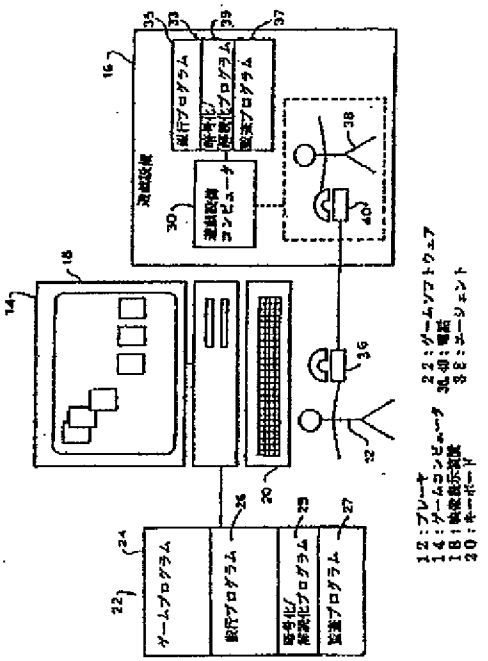
審査請求　未請求　請求項の数31　OL　（全 24 頁）

(21)出願番号　特願平7－19207
(22)出願日　平成7年(1995)2月7日
(31)優先権主張番号　08／212348
(32)優先日　1994年3月11日
(33)優先権主張国　米国（US）
(31)優先権主張番号　08／269248
(32)優先日　1994年6月30日
(33)優先権主張国　米国（US）

(71)出願人　595018905
ウォーカー・アセット・マネジメント・リミテッド・パートナーシップ
WALKER ASSET MANAGEMENT LIMITED PARTNERSHIP
アメリカ合衆国，コネティカット州，ニュー・キャナーン，エルム・ストリート 125
(72)発明者　ジェイ・ウォーカー
アメリカ合衆国，コネティカット州，リッジフィールド，スペクタクル・レーン 124
(74)代理人　弁理士　曾我　道照　（外6名）

(54)【発明の名称】　遠隔ゲーム装置，ゲームコンピュータ、ゲーム方法およびゲーム装置

(57)【要約】
【目的】　遊戯設備と関連したホストコンピュータとオンライン接続を確立することを要さない場合にパーソナルコンピュータまたはポータブルコンピュータで遠隔地から遊戯設備または宝くじに対してプレーヤがゲームをできる遠隔ゲーム装置を得る。
【構成】　ゲームコンピュータは少なくとも1つのゲームの機会を提供し、プレーヤにクレジットを取得しかつ任意の結果として得た賞金を現金化する。ホストコンピュータはプレーヤおよび遊戯設備間の一連の暗号化されたコード交換を通して遠隔地でプレーヤにクレジットの購入および買い戻しをさせる。また、パーソナルコンピュータで使用するためのゲームコンピュータまたはクレジットモジュールが予め装備されたクレジットを有するプレーヤに提供される。また、ゲーム装置は、結果が不確定な未来の出来事例えば宝くじに関係可能とし、それにより、プレーヤは遠隔地でゲームコンピュータでの選択をする。



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 684 575 A1**

(12) **EUROPEAN PATENT APPLICATION published in accordance with Art. 158(3) EPC**

(21) Application number: 95902954.7

(51) Int. Cl.: G06F 19/00

(22) Date of filing: 14.12.94

(86) International application number:
PCT/JP94/02099

(87) International publication number:
WO 95/16970 (22.06.95 95/26)

(30) Priority: 14.12.93 JP 313246/93

(43) Date of publication of application:
29.11.95 Bulletin 95/48

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(71) Applicant: MOCHIDA PHARMACEUTICAL CO., LTD.
7, Yotsuya 1-chome
Shinjuku-ku
Tokyo 160 (JP)

(72) Inventor: YAMAUCHI, Tadakazu
Mochida Pharmaceutical Co., Ltd.
7, Yotsuya 1-chome
Shinjuku-ku
Tokyo 160 (JP)

(74) Representative: Casalonga, Axel et al
BUREAU D.A. CASALONGA - JOSSE
Morassistrasse 8
D-80469 München (DE)

(54) **MEDICAL MEASURING APPARATUS.**

(57) A medical measuring apparatus which enables a person to be inspected, such as patients and pregnant women and an attendant or the like, to perform a variety of medical measurements at home or the like. The apparatus enables a person such as a physician having a specialized knowledge to specify a person to be inspected, set measuring items, criterions and comments and commands, which are based on measurement results, in accordance with the condition of a disease, physical condition and constitution of an individual person to be inspected, circumstances or the like, and to execute judgment for the measurement results in accordance with the set criterions or the like and output comments and execute commands, and a person to be inspected to uses these comments and the results of commands, in accordance with the measurements results.

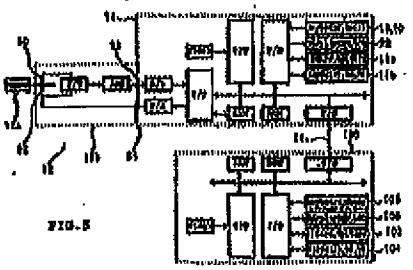


FIG. 5

EP 0 684 575 A1

TECHNICAL FIELD

The present invention relates to a medical measurement apparatus for allowing not only medical experts but also patients, pregnant women and their attendants or helpers to readily perform medical measurement in medical institutions or elsewhere (e.g., at home). More particularly, the invention relates to a medical measurement apparatus which permits health-care or medical experts such as doctors to identify the subject such as a patient or a pregnant woman and to set appropriate comments about that subject with respect to relevant measuring items, to the criteria for judgment and to the measured results, the comments being utilized by the subject depending on the measured results.

The medical measurement apparatus of this invention allows medical measurement to be made by patients or pregnant women themselves as well as by their attendants or helpers. As a matter of convenience, the specification hereunder will refer to the patient, pregnant woman, etc. from whom to collect specimens as "the subject," and the person operating the inventive medical measurement apparatus for measuring the collected specimens as "the operator." The subject and the operator may or may not be the same person.

BACKGROUND ART

A large number of medical measurement systems and apparatuses have been developed for easy use by the patients, pregnant women or their attendants carrying out various kinds of medical measurement on their own. The measurements include such items as blood pressure, urine sugar level, urine protein and occult blood, as well as pregnancy tests and observation of mothers' conditions.

Many of the conventional systems and apparatuses utilize test liquids and test paper. In operation, such testing agents require visually inspecting the change in color tone dependent of the amount of the target analyte detected in specimens, whereby the measurements are determined.

Recent years have seen the advent of many other apparatuses that convert an optically measured color tone change into electrical signals or turn the target analyte amount (i.e., concentration) in the specimen into electrical signals. The signals thus obtained are used as the basis for computing measurements that are displayed numerically and/or graphically on a display unit (see Japanese Patents Laid-Open Nos. Sho 61-83944, Sho 63-61157, etc.).

Some medical measurement systems performing electrical measurement store measured results in the past on a number of occasions and allow them to be retrieved later and displayed as needed to make more accurate medical measurement and diagnosis. Other systems comprise a mechanism that generates an alarm if the measuring conditions such as temperature and the target analyte concentration in the specimen are not appropriate (see Japanese Patents Laid-Open Nos. Sho 63-167040, Sho 61-47555, etc.).

Japanese Patent Laid-Open No. Hei 6-266851 discloses a body temperature data management system comprising a clinical thermometer equipped with an LED. When the LED on the clinical thermometer blinks to generate digital signals representing body temperature measurements of the subject on a time series basis, the system properly reads the optical signals to have the body temperature data transferred thereto in a cord-free environment. The body temperature data is stored along with ID information on the subject and the time stamps of measurement, to be displayed later graphically or otherwise on a display unit.

The majority of the conventional medical measurement systems and apparatuses have their measuring items fixedly determined beforehand, and numerically display such diverse measurements as urine sugar level and blood pressure. The judgment on the measured results is entrusted to the operator (i.e., subject) who may have no specialized knowledge of the field in question.

Some systems have the ability to judge and indicate that a particular measurement is excessively high or low (too large, too small, etc.) relative to the relevant standard range (see Japanese Patent Laid-Open No. Sho 61-73055). However, such judgments are set generally for all subjects; judgments tailored to individual subjects cannot be performed.

If the medical measurement systems with a measurement storage feature measure irrelevant subjects or perform measurement under faulty ambient conditions, such measurements are still stored unchecked. When viewed later by doctors and other experts, totally irrelevant measurements can be taken as valid clinical data, which can result in misdiagnosis.

The above-cited body temperature data management system disclosed in Japanese Patent Laid-Open No. Hei 6-266851 has the function of managing body temperature data based on the ID information about specific subjects. This system, too, simply measures body temperatures and stores the measurements in a fixed manner. The system has no capability for making appropriate and fine-tuned judgments tailored to individual subjects on the basis of their body temperature data.

In recent years, various forms of remotely provided medical care (generally called home care) have been on the rise. In particular, patients with chronic diseases or in the chronic stage of their disorders are often taken care of at home and not in the hospital, with a view to improving the quality of life for the patients. For example, patients who are bedridden due to cerebral disorders or because of their advanced ages, patients with chronic nephritis, diabetes, cancer, coronary and hepatic disorders, infertile women, and pregnant women are fit to receive home care. These home-care or self-managing patients live outside medical institutions and thus require more adequate and rigorous supervision by doctors and other experts than in-patients. The home-care patients are apt to become anxious about their conditions, and the doctors and experts in charge of these patients are required to spend much more time on them than on in-patients in terms of remotely conducted examination and consultations by telephone. Because of the current constraints on the number of doctors and experts and on the facilities available for home care, there is an urgent need for medical care management technology for caring individual patients efficiently, appropriately and in an individually customized manner.

The conventional techniques are capable of managing a large number of patients in a fixed manner, but are incapable of establishing or modifying the measuring conditions, the criteria for judgment, or corresponding remedies and treatments for individual patients. Because important judgments are left for the patient to make, it is difficult for the experts managing the system to deal with sudden changes in the patient's conditions quickly and adequately. Although there exist means of communication and data transfer systems which the doctors or experts may use to manage and transfer the measured data on patients in remote locations, the fact remains that the doctors or experts in charge must keep constant surveillance over the data on numerous patients. Despite the dedicated facilities and human resources, the patients are unable to feel reassured that they are adequately taken care of based on their measured results. The means and systems for communicating and transferring measured data between remote locations are apparently effective in reducing the number of times each patient visits the hospital or the number of times the patient is personally examined by the doctor. However, what these facilities can do is simply to replace the hospital visits or the examinations in hospital with transfers of data or judgments on those data remotely made. There have yet to be solutions to the problems of how to reassure both the patient and the doctor about the effectiveness of home care while alleviating the burdens on both of them in a home-care environment.

One solution to such problems is a home care support system that connects patients' terminals with a central control unit via means of communication (as disclosed in Japanese Patent Laid-Open No. Hei 4-16095). This system, dependent on computer-based communications, requires its central control unit to judge information input through the patients' terminals (ID inquiry, measured data, answers to questions) and to transmit the judged results to the terminals. If the means of communication becomes faulty or unavailable, measuring operations may not be carried out or the judged results may not be transmitted. This can cause serious medical problems to patients who must take emergency measurements or who need continuous testing. Furthermore, the system does not allow the doctor to manage individual patients on the basis of time information (i.e., time stamps of measurements) or of the measuring items. Because unnecessary or irrelevant measurements cannot be excluded, the system is incapable of administering home care effectively.

DISCLOSURE OF THE INVENTION

It is therefore an object of the present invention to overcome the above and other deficiencies and disadvantages of the prior art and to provide a medical measurement apparatus allowing the subject such as patients and pregnant women or their attendants to conduct various kinds of medical measurement at home or elsewhere outside medical institutions. With the subject identified and with the individual's symptoms, physical conditions, constitution and environment verified, a doctor or a medical expert with specialized knowledge sets to the apparatus the measuring items, the criteria for judgment, and comments and/or commands corresponding to the measured results. Given the criteria and other relevant items, the apparatus outputs judgments on the measured results, and issues appropriate comments and executes commands in keeping with such judgments. The subject can then make effective use of such comments and the result of command execution in accordance with the measured results.

In achieving the foregoing and other objects of the present invention and according to one aspect thereof, there is provided a medical measurement apparatus comprising a measuring unit for outputting electrical signals in accordance with the amount of a target analyte measured in a specimen, and a control unit. The control unit includes: identification means for receiving identification data specific to a subject and for identifying that subject on the basis of the identification data; criterion setting means only for use by a

controller who sets comments about measured results regarding the measuring items and the criteria set for the subject and who is capable of making a specialized judgment on the amount of the target analyte in the specimen; and judgment and display means for computing the measurements based on the electrical signals from the measuring unit and for selectively displaying the comment relevant to the criteria with respect to the computed measured results.

In a preferred structure according to the invention, the identification data is set only by the controller.

In another preferred structure according to the invention, the control unit includes storage means for storing a plurality of measurements, and the controller retrieves the stored measurements as desired.

In a further preferred structure according to the invention, the storage means stores the measurements with respect to which the criteria are modified as needed.

In an even further preferred structure according to the invention, the control unit includes either or both of questioning means and verification means, the questioning means being used to put preliminary questions to the subject in connection with the measuring items, the verification means being utilized to verify that measurement is performed under the measuring conditions established in accordance with the measuring items, and only the controller is allowed to set the preliminary questions and the measuring conditions.

In a still further preferred structure according to the invention, the control unit includes time stamp setting means for setting timer-counted time stamps to be measured in keeping with the measuring items, and time stamp verification means for verifying that a given measurement was taken at the correspondingly set time of day, and only the controller is allowed to set the time stamps.

In a yet further preferred structure according to the invention, the criterion setting means in the control unit is arranged to set commands either in place of or in conjunction with the comments, and the judgment and display means is either replaced with or supplemented by judgment execution means for selectively executing the commands.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a conceptual view of an example of the medical measurement apparatus practiced as the preferred embodiment of the invention;

Fig. 2 is an example of the circuit diagram of the output section in the measuring unit of the embodiment in Fig. 1;

Fig. 3 is a schematic exploded perspective view of an example of the analyzing section in the measuring unit of the embodiment in Fig. 1;

Fig. 4 is a cross-sectional view of the analyzing section in Fig. 3 as it is assembled;

Fig. 5 is a schematic view showing an example of typical signal connections between the measuring unit and the control unit of the embodiment;

Fig. 6 is a flowchart of an example of typical steps carried out by the controller of the embodiment;

Fig. 7 is a flowchart of an example of typical steps performed by the operator of the embodiment;

Fig. 8 is another flowchart of an example of typical steps carried out by the controller of the embodiment;

Fig. 9 is another flowchart of an example of typical steps conducted by the operator of the embodiment;

Fig. 10 is another flowchart of an example of typical steps followed by the controller of the embodiment;

Fig. 11 is another flowchart of an example of typical steps carried out by the operator of the embodiment;

Fig. 12 is another flowchart of an example of typical steps conducted by the controller of the embodiment;

Fig. 13 is another flowchart of an example of typical steps performed by the operator of the embodiment;

Fig. 14 is a schematic view of an example of the typical display (on the control panel) in effect when the controller starts making entries into the embodiment of Fig. 1;

Fig. 15 is a schematic view of an example of the typical display (on the control panel) in effect when the controller sets measurements in the embodiment;

Fig. 16 is a schematic view of an example of the typical display (on the control panel) in effect when the operator starts making measurement using the embodiment;

Fig. 17 is a schematic view of an example of the typical display (on the control panel) in effect when the operator terminates measurement with the embodiment;

Fig. 18 is a conceptual view depicting how the controller operates the embodiment and how the control unit of the embodiment acts in response; and

Fig. 19 is a conceptual view showing how the operator operates the embodiment and how the control unit of the embodiment acts in response.

BEST MODE FOR CARRYING OUT THE INVENTION

The preferred embodiment of the invention will now be described with reference to the accompanying drawings.

Fig. 1 is a conceptual view of a medical measurement apparatus practiced as the preferred embodiment of the invention.

The medical measurement apparatus 10 in Fig. 1 is one which allows not only health-care professionals such as doctors and nurses but also the subject such as patients, pregnant women and their attendants to readily perform medical measurement (testing) in medical institutions or elsewhere (e.g., at home). As illustrated, the medical measurement apparatus 10 primarily comprises a measuring unit 12 and a control unit 14 that receives data from the measuring unit 12 so as to output and display measurements. The control unit 14 includes a control unit body 16, and input means such as a keyboard 18 and a mouse 20 used to input various conditions and the subject's ID data to the system. The control unit body 16 is equipped with a display unit 22 that displays measured results and various comments.

The control unit 14 further comprises a drive unit 28 that writes and reads data to and from a storage medium for preserving measured results and personal information. The storage medium may be a floppy disc, a hard disc, an optical disc, a magneto-optical disc, an IC card, an IC memory card, an optical card or a magnetic card. The control unit 14 has a communication line 24 connected as needed to a host computer or a server at the controller's site in medical institutions. The drive unit 28 may be incorporated in, or attached externally to (or auxiliary), the control unit 14.

The input means of the invention may be something other than the keyboard 18 or mouse 20 illustrated; it may be a push button arrangement, a pen input device, a touch panel or a voice input unit. The input means may utilize a storage medium such as a magnetic card, an IC card, an optical card, an IC memory card or a floppy disc. All known input means may be usable with the invention. The display unit 22 may be an LCD, a CRT unit or a voice output unit, or it may be a hard copy output device such as a printer. The display on the screen may include not only characters but also pictures including animations.

A plurality of input means and display means may be provided in suitable combination. For example, operating instructions, entry prompts and/or experts' comments may be displayed in characters and pictures or may be output in voice. Such arrangements will make the operation of the apparatus easier and subject to fewer errors. When comments are printed out in hard copy, they can be preserved for later use by the operator.

The measuring unit 12 has a section for taking measurements of the subject's specific parts, a section for receiving a specimen collected from the subject, or a section for accommodating test paper or a sample holder containing the specimen. With measurements taken, the measuring unit 12 outputs electrical signals representative of the subject's measuring item or of the amount of the target analyte in the specimen. In Fig. 1, the measuring unit 12 is composed of an analyzing section 12a such as a sensor chip and of an output section for converting the output from the analyzing section 12a into electrical signals for output to the control unit 14.

The analyzing section 12a may be either incorporated beforehand in the output section 12b, or may be attached (i.e., loaded) to the output section 12b at the time of measurement.

The medical measurement apparatus 10 of the invention is not limited in terms of the way in which the measuring unit 12 (analyzing section 12a) generates (outputs) signals representing the amount of the target analyte in the specimen, i.e., in the way the target analyte amount is measured. Any known specific analysis methods may be utilized. Preferably, the measuring unit 12 should make use of immunoassay, nucleic acid assay, ligand-receptor assay or the like. The most preferred method of analysis is immunoassay.

Specific reactions of the target analyte under test may be obtained and reaction-caused changes may be detected with the apparatus. In such cases, a conductivity meter is used if changes are caused in conductivity by reaction; a potentiometer is used if potential differences are brought about by reaction; a potentiostat, a coulomb meter, an ammeter or other appropriate electrical measuring device is used if the reaction involved is an electrochemical reaction; a fluorometer is used if the reaction entails fluorescence; a luminometer is used if the reaction is accompanied by luminescence; and a color-difference meter, a photometer or a reflectometer is used if the reaction involves coloration. Preferably, the electrical measuring device should be employed.

Fig. 2 is a circuit diagram of the output section 12b in the measuring unit 12 of the embodiment, the output section 12b generating electrical signals representing the amount of the target analyte detected in the subject's specimen through electrochemical reaction. A WE terminal 30 and a CE terminal 32 are connected respectively to a working electrode and a counter electrode terminal of the analyzing section

12a. A D/A terminal 34 and an A/D terminal 36 are connected respectively to a digital-analog (D/A) conversion circuit terminal and an analog-digital (A/D) conversion circuit terminal of the control unit 14. With this embodiment, the D/A and A/D conversion circuits are located in a multi-function data I/O board AT-MIO-16X (from National Instruments) housed in the control unit body 16. The example of Fig. 2 constitutes a potentiostat circuit. The potential output by the control unit 14 via the D/A terminal 34 is applied between the working electrode and counter electrode terminals of the analyzing section 12a. A current flows through the working electrode terminal of the analyzing section 12a in response to the amount of the target analyte in the specimen. The detected current is converted to a potential by a current-potential conversion circuit, and the potential is amplified by an amplifier circuit to form electrical signals that are sent to the control unit 14 via the A/D terminal 36.

The control unit 14 computes values form the received electrical signals. The computed values are compared with criteria that have been set beforehand by the controller for the subject in question. The control unit 14 then outputs a controller-predetermined judgment on the measured results, or output comments or executes commands in keeping with the judgment.

The analyzing section 12a that generates electrical signals representing the ampunt of the target analyte in the subject's specimen through electrochemical reaction may be any one of diverse sensors including an enzyme sensor, an immunosensor, a nucleic acid sensor, a microorganism sensor, a biosensor, a chemical sensor, a semiconductor sensor and a gas sensor (A.P.F. Turner, I. Karube and G.S. Wilson, Biosensors - Fundamentals and Applications, 1987; Electrochemical Sensors in Immunological Analysis, 1987; E.A.H. Hall, Biosensors, 1990).

Below is a description of an analyzing section adopting an electrochemical enzyme immunoassay technique known as MEDIA (mediator diffusion-controlled immunoassay), as disclosed in Japanese Patent Laid-Open No. Hei 5-264552. Figs. 3 and 4 are schematic views of such an analyzing section 12a.

This type of analyzing section 12a employs urine as specimen liquid to assay the quantity of urine hCG (human chorionic gonadotropin). The result of the assay is used for diagnosis of pregnancy.

The analyzing section 12a has an acrylic lower plate 68 supporting an absorber 64 in the form of a round cellulose filter paper (12 mm diameter) impregnated with a mixture of hydrogen peroxide and urea and freeze-dried. As illustrated, the absorber 64 has a sealing portion 64a on the upper side surface of the absorber 64 (this side will be regarded as the face and the other side as the back). The sealing portion 64a of a round, liquid-impermeable seal (6 mm diameter) is pasted on the central portion of the upper side surface of the absorber 64.

Above the absorber 64 is a stack of round, porous, anti-hCG antibody-insolubilized membrane 62 (13 mm diameter).

An electrode plate 60 is placed on top of the antibody-insolubilized membrane 62. The electrode plate 60 is made of a PET film (16 x 44 mm). The face and the back of the PET film have a ring-like silver electrode (6 mm in outer diameter, 3 mm in inner diameter) and a ring-like carbon electrode (6 mm in outer diameter, 3 mm in inner diameter) screen-printed respectively thereon, the two electrodes being axially aligned. Thus the electrode plate 60 has the ring-like shaped silver printed electrode (counter electrode 72) on its face and the ring-like shaped carbon printed electrode (working electrode 74) on its back. A counter electrode terminal 72a and a working electrode terminal 74a are connected respectively to the counter electrode 72 and the working electrode 74. Conductors other than the ring-like shaped electrodes (72 and 74) and the terminals (72a and 74a) are covered with resist ink and are not exposed. The electrode plate 60 also has a through hole 70 (3 mm diameter) that penetrates the center of the two electrodes. The electrode plate 60 is mounted so that the through hole 70 is aligned axially with the antibody-insolubilized membrane 62. The through hole 70 is filled with a connecting part 58 made of a round, glass fiber filter paper (3 mm diameter).

On top of the electrode plate 60 is placed a round, glass fiber filter paper 56 (12 mm diameter) treated by surface active agent. The filter paper 56 is axially aligned with the through hole 70. A round, liquid-impermeable seal (6 mm diameter) is pasted as a sealing part 56a onto the center portion of the surface of the glass fiber filter paper 56.

Over the glass fiber filter paper 56 is an enzyme labeled antibody-impregnated part 54 axially aligned with the filter paper 56 below. The enzyme labeled antibody-impregnated part 54 has peroxidase enzyme labeled anti-hCG antibody solution impregnated in a round glass fiber filter paper (12 mm diameter) and freeze-dried therein. A round, nonwoven fabric portion (12 mm diameter) is further placed as a filter part 52 onto the enzyme labeled antibody-impregnated part 54.

The analyzing section 12a is topped with an acrylic upper plate 50 having a specimen inlet port 50a (6 mm diameter). The specimen inlet port 50a of the upper plate 50 is axially aligned with the filter part 52 below. The analyzing section 12a is assembled by screwing the upper plate 50 to the lower plate 66.

For analysis, the working electrode terminal 74a conducting to the working electrode 74 of the analyzing section 12a is connected to the WE terminal 30 of the output section 12b; the counter electrode terminal 72a conducting to the counter electrode 72 is connected to the CE terminal 32 of the output section 12b. Alternatively, the analyzing section 12a and output section 12b may be integrated so that the working electrode terminal 74a and the counter electrode terminal 72a double respectively as the WE terminal 30 and the CE terminal 32.

The operator introduces a urine specimen together with an electron mediator compound such as p-benzoquinone into the specimen inlet port 60a of the analyzing section 12a. Measurement is started by the operator pushing a measurement start button on the control unit 14, to be described later.

With measurement started, the control unit 14 causes the output section 12b to apply a potential of -200 mV between the working electrode 74 (terminal 74a) and the counter electrode 72 (terminal 72a) of the analyzing section 12a, and measures the reduction current through the working electrode 74 every second. Current measurements taken over three to five minutes following the start of measurement are averaged. The average is put into standardized relational functions incorporated in advance into the arithmetic processing mechanism in the control unit 14, whereby the hCG concentration in the specimen is computed. The computed value is compared with the criteria established by the controller in the control unit 14.

The liquid specimen introduced into the analyzing section 12a in the manner described passes through the filter part 62 that removes aggregates and other impurities from the liquid. The specimen liquid then dissolves the enzyme labeled antibody of the enzyme labeled antibody-impregnated part 64, bypasses the sealing part 66a and flows into the glass fiber filter paper 66. During that time, the hCG antigen in the specimen liquid is bound with the enzyme labeled antibody to form an antigen-enzyme labeled antibody complex. The liquid specimen further passes through the connecting part 68 and the through hole 70 of the electrode plate 60 to enter the antibody insolubilized membranes 62, bypassing the sealing portion 64a below. The liquid penetrates through the antibody insolubilized membranes 62 radially from the center to the periphery, to be absorbed into the absorber 64 to dissolve a sufficient amount of enzyme substrate therein.

While the specimen liquid is penetrating through the antibody insolubilized membrane 62 radially, the antigen-enzyme labeled antibody complex mentioned above is further bound with an insolubilized antibody to form a sandwich type complex (insolubilized antibody-antigen-labeled antibody complex). For this to take place, the antibody insolubilized membrane 62 have a distribution of the labeling enzyme formed in accordance with the amount of the antigen by the sandwich-type binding to the labeled antibody and the insolubilized antibody. That is, the greater the amount of the antigen in the specimen liquid, the more localized the labeled enzyme toward the center of the round antibody insolubilized membrane 62. Conversely, the smaller the amount of the antigen in the specimen liquid, the more dispersed the labeling enzyme throughout the antibody insolubilized membrane 62.

In the analyzing section 12a utilizing the MEDIA method, the electron mediator mediates between the ring-like shaped working electrode 74 contacting the center portion of the antibody insolubilized membranes 62 on the one hand, and the labeling enzyme distributed in the antibody insolubilized membrane 62 on the other hand. Through mediation of the electron mediator, the oxidation reduction reaction of the labeling enzyme is measured as a current. In the example above, p-benzoquinone (i.e., electron mediator) mediates recyclically between the reaction of peroxidase (labeling enzyme) with the hydrogen peroxide substrate on the one hand, and the electrode reaction of the working electrode 74 on the other. In this setup, the reduction current of the electron mediator caused by the electrode reaction at the working electrode 74 is measured. The reduction current whose intensity depends on the mass transfer through diffusion of the electron mediator is significantly affected by the distance distribution between the labeling enzyme molecules and the working electrode 74. Thus the larger the number of labeling enzyme molecules localized toward the center of the antibody insolubilized membranes 62 due to a high amount of the antigen in the specimen, the larger the current. Conversely, the more dispersed the labeling enzyme molecules throughout the antibody insolubilized membranes 62 due to a low amount of the antigen in the specimen, the smaller the current. It follows that with standardized relational functions obtained by prior analysis of specimens containing the antigen of standard concentration, the concentration of the antigen in the specimen in question is computed from the current value in the form of electrical signals.

Described above is the example in which the measuring unit 12 made of the analyzing section 12a and output section 12b utilizes electrochemical reaction. Alternatively, any other method or means for generating electrical signals reflecting the amount of the target analyte in the specimen may be used as the measuring unit 12 of the medical measurement apparatus embodying the invention.

The signals from the measuring unit 12 (i.e., measurements obtained by the measuring unit 12) are sent to the control unit 14.

As illustrated, the control unit 14 comprises the control unit body 16 having the display unit 22, the keyboard 18, and the mouse 20 that may be attached as needed. Given the signals from the measuring unit 12, the control unit 14 computes the measured results and displays the measured results on the display unit 22 along with relevant comments. The control unit 14 may also execute commands in accordance with the acquired measurements. The control unit body 16 is a processing unit incorporating a microprocessor. The processing unit should preferably a computer or the like in view of versatility and expandability. This embodiment utilizes the lap-top computer Portable 486c (from Compaq) that is partially expanded. The above-described measuring unit may be either incorporated in the control unit body 16 or attached thereto externally.

The control unit 14 is not limited to a computer. It may be any device which permits the use of a processing unit, a storage unit, a display unit and an input unit and which connects to or incorporates a measuring unit. Another alternative is to integrate the control unit and the measuring unit.

A major application of the inventive medical measurement apparatus is found in the situation of remotely provided medical care such as a home-care setup. Typical configurations of the apparatus for remotely provided medical care will now be described.

Where the control unit 14 of the measuring unit 12 is made portable, the controller such as a doctor stores the criteria for judgment and the comments or commands about the acquired measured results with respect to the criteria into the storage means of the control unit 14, and hands the control unit 14 over to the operator. The storage means in the control unit 14 may be any one of a backed-up RAM, a hard disc, a magneto-optical disc, a floppy disc, an IC card, an IC memory card, an optical card and a magnetic card. The operator carries the control unit 14 home or somewhere outside for measurement, takes measurements on the spot, and acts on the results using the criteria and comments or commands established by the controller. When paying a visit to the controller, the operator carries with him the control unit 14. The controller then retrieves the measurements from the storage means for reference. Such stored measurements may be used not only as information by which the operator or the subject has a better understanding of his pathologic condition, but also as information according to which the controller diagnoses the subject. Depending on the circumstances or condition of the subject, the controller may modify the criteria or the comments or commands regarding the measurements with respect to the criteria, store the modifications in the storage means of the control unit 14, and hand the control unit 14 back to the operator.

Even where the control unit 14 is not arranged to be portable, the controller such as a doctor may modify the criteria or the comments or commands regarding the measurements with respect to the criteria, store the modifications into portable storage means of the control unit 14 via the host computer or server, and hand the storage means back to the operator. The portable storage means may be any one of an IC card, an IC memory card, an optical card, a magnetic card, a floppy disc, a hard disc card, an optical disc and a magneto-optical disc (MO). For measurement, the operator connects the storage means to the control unit 14 located at home or somewhere outside, takes measurements on the spot, and acts on the results wherever he is by use of the criteria and comments or commands established by the controller. The measured results are stored into the storage means. When paying a visit to the controller, the operator carries with him the storage means. The controller then retrieves the measurements from the storage means for reference using the control unit body as the host computer. Depending on the circumstances or condition of the subject, the controller may modify the criteria or the comments or commands regarding the measured results with respect to the criteria, store the modifications into the storage means, and hand the storage means back to the operator.

In the above configurations of the apparatus, fine-tuned diagnostic settings are available for individual subjects. In that case, both the controller and the subject feel reassured that the subject is being properly cared for under the controller's supervision. It is then possible for the measured results to be judged quickly according to the controller-established criteria so that relevant comments or commands prompt the operator or the subject to take appropriate action or to suppress unnecessary behavior. As a result, the burdens on the controller, the operator and the subject are all alleviated.

Another application of this apparatus is a configuration comprising communication lines or networks. In this case, the control unit 14 is composed of a control unit body acting as the host computer or server, and of one or a plurality of terminals or clients each including a measuring unit 12. This system configuration connects the host computer or server on the controller's side with the subject's terminal or client using a communication line 24 or the like. The controller may then take note of the subject's pathologic condition in real time, issue appropriate instructions and/or take relevant action accordingly.

In a relatively restricted area such as inside the hospital, a LAN setup illustratively based on the Ethernet may be used for communication purposes. Where remote locations are involved, a leased line network or a public network may be employed. The communication line may be either a physical line such

as a telephone line or wireless circuits such as those utilizing a communication satellite.

Fig. 5 is a schematic view showing typical signal connections between the measuring unit 12, the control unit 14 and a host computer or server 100. The storage means of the control unit 14 or that of both the control unit 14 and the host computer or server 100 accommodates a group of control commands for controlling the measuring unit 12 during measurement, the criteria for judgment established by the controller, and comments and commands about the measured results with respect to the criteria. The storage means may be any one of a ROM, a backed-up RAM, a card medium 16a and 102 such as an IC card, an IC memory card, an optical card and a magnetic card; and a storage medium 16b and 104 such as a hard disc, a magneto-optical disc, a floppy disc, a magnetic tape and a DAT. In Fig. 5, reference numeral 106 indicates input means such a mouse and a keyboard of the host computer or server 100, and reference numeral 108 is a display unit of the host computer or server 100.

Below is an example in which the controller establishes various diagnostic settings using the host computer or server 100, with a remotely located operator using the control unit 14 for measurement and medical care via the communication line 24.

For this example, it is assumed that at least the control unit 14 stores a group of control commands for controlling the control unit 14.

When the operator starts the control unit 14, a group of control commands is retrieved from the storage means of the control unit 14 to control the control unit 14. With measurement completed, the measured results are written to the storage means of the controller's host computer or server 100 and/or to the storage means of the control unit 14. Where necessary, the controller may retrieve for reference the measurements from the storage means of the host computer or server 100. On the basis of the measured results, the controller may operate the host computer or server 100 to modify as needed the criteria for judgment as well as the comments and/or commands about the measurements with respect to the criteria. The above scheme allows the control unit 14 to make measurement even if the communication line becomes faulty. Thus the scheme is safe and preferable.

The measured results may be stored in one or both of the two storage means: one for the control unit 14 on the operator's side, the other for the host computer or server 100 on the controller's side. The measured results may include computed values regarding the target analyte in the specimen, the operator's name, the operator code, the subject's name, the subject code, dates of measurements, time stamps of measurements, and the operator's answers to preliminary questions. Where storage addresses and storing methods are standardized, the subject or operator may receive individual supervision concurrently from a plurality of controllers. If the measured results are written to the storage means of the control unit 14, the subject or the operator can readily reference his past measurements therefrom. This is preferable in terms of better self-care. In particular, the storage means is preferably detachable, such as the card medium 16a (e.g., IC card), floppy disc or the like. Such storage means will allow the subject or the operator to utilize advantageously a plurality of control units 14 (at home, in the office, etc.). Because the subject or the operator can readily handle the portable card or like medium on his own, the subject or the operator finds it easy to manage his own medical data. This aspect of individual data management is desirable in view of protection of privacy. Furthermore, the easy handling of the storage medium makes it easier for a plurality of subjects and operators to share a single control unit 14.

On the other hand, if the measured results are written to the storage means attached to the host computer or server 100, the controller such as a doctor may build the pathologic conditions of a plurality of subjects (e.g., patients) illustratively into a database for collective supervision, which is desirable for better health care from the controller's viewpoint. For this to be implemented, the measurements may be written both to the storage means of the control unit 14 and to the storage means of the host computer 100. For efficient communication, the measured results may preferably be transferred in batch form to the host computer or server when data transfer is requested by the controller, when the measured results have reached a threshold level (to trigger a command), or when the storage means of the control unit has become full. Under certain circumstances, it is also preferable to trigger data transfer depending on the answer to a preliminary question. Any or all of the above alternatives may be selected in consideration of the pathologic conditions of the subject to be supervised, the life styles of the controller and of the subject, and the costs involved (communication costs in particular). If the communication means develops failure rendering the communication unavailable, the settings and the measurements are still held in the storage means of the control unit 14. In that case, there is no problem with measurement and judgment on the part of the control unit 14.

The above-mentioned connection based on the communication line can afford additional benefits to the medical measurement apparatus of the invention. For example, in a home-care situation, it is important to respect the patient's right to know. In particular, a self-managing patient should preferably be encouraged to

take part actively in the performance of medical care so as to gain better therapeutic results. With this apparatus, too, it is desirable for information about the controller-set measuring items and criteria to be made available to the subject or operator upon request. Illustratively, the control unit in the operator's possession may be connected via a communication line to such data sources as an externally furnished database and a database housed in the host computer or server on the part of the controller. Such a setup allows the subject or operator to retrieve information about the relevant examination or medical care from the control unit. The retrievable information may include the content of the examination (i.e., purpose of the examination), the examination method (the manner in which the examination is to be performed), and criteria for judgment (normal values). Information may be retrieved from the data sources by use of commands set by the controller. Whereas it is feasible to incorporate in the control unit a data source in the form of, say, CD-ROMs, a wider range of applications is available when the subject or operator is allowed to have access via a communication line or network to an external data source.

It should be noted that, as mentioned above, the measurement, judgment and other functions of the control unit 14 do not presuppose the presence of the communication line 24.

The control unit 14 (control unit body 16) of the above constitution comprises: identification means for identifying the subject of measurement; criterion setting means only for use by the controller such as a doctor who is capable of making a specialized judgment on the amount of the target analyte in specimens by use of specialized knowledge about the measured results; and judgment and display means for computing measurements based on the output signals from the measuring unit 12 and for selectively displaying relevant comments about the computed measurements. Preferably, the medical measurement apparatus 10 has storage means for storing a plurality of measurements, questioning means for putting preliminary questions to the subject (operator), and verification means for verifying that measurement is performed under appropriate conditions.

The identification means is a function that identifies the subject of measurement based on his identification data supplied by the operator.

Equipped with this identification means, when the medical measurement apparatus 10 of the invention allows only the identified subject, no other subjects are examined and the apparatus is arranged to accumulate measurements of only the identified subject(s).

When the medical measurement apparatus 10 deals with a plurality of subjects, the apparatus is constituted to take measurements specific to each of the individual subjects. If unnecessary measurements are taken of any subject, they cannot be examined by the apparatus and only the relevant measurements are accumulated with respect to the individual subjects.

Thus the inventive medical measurement apparatus 10 does not mix measurements of one subject with those of any other subject. With the possibility of mixed-up measurements eliminated, the controller such as the doctor is not misled to make erroneous diagnosis based on the incorrectly accumulated measurements.

The medical measurement apparatus 10 of the invention poses no specific constraints on the types of usable identification data about the subject. The identification data may preferably include personal data such as the name and the date of birth, the ID code such as a password number, the fingerprint and the voice print of each subject. The identification may be provided alternatively in the physical form of a security card or a key possessed by the subject or by the operator. No specific constraints exist on the manner of entering the identification data. That is, the ID data may be input by use of the keyboard 18, the mouse 20, a touch panel, a bar code reader, a card reader for reading ID cards, a magnetic cards or optical cards; or a disc drive for driving floppy discs, magneto-optical discs or hard discs.

In other words, the embodiment of the invention may utilize advantageously any of the diverse means of personal identification. However, it is preferred that the apparatus should be made unavailable for measurement unless and until both an ID card (e.g., security card) and a password code are entered. The health insurance card, driver's license, electronic medical chart or other personal identification card of the subject may use as his ID card or security card. Alternatively, the ID card may be a card issued by the controller at the time of registering the patient with the apparatus.

For the medical measurement apparatus 10 of the invention, the identification data should preferably be set by the controller alone. To have the settings of the apparatus established only by the controller requires two things: either the controller alone is allowed to make or modify the settings, or only the subject or operator authorized by the controller is to carry out the same.

These arrangements are intended to prevent the operator or any other third party from inadvertently altering the identification data or from making other careless or deliberate modifications of data.

There are no specific constraints on the manner in which to set identification data. The same methods as those cited above for entering the ID data may be utilized.

Similarly, there exist no specific limits to the way in which to limit the qualification for setting ID data only to the controller. Any one of various known methods for entering the subject's identification data such as the use of the controller's ID code may be utilized.

The criterion setting means is used only by the controller such as a doctor who has specialized knowledge on medicine and who sets the items of measurement, the criteria for judging measured results, and comments and commands about the measurements with respect to the criteria. The settings can be made for each individual subject and in consideration of the changes over time in the subject's conditions.

To make effective use of the measurements taken by the medical measurement apparatus requires selecting appropriate measuring items by taking into account the patient's pathologic conditions and symptoms, the result of the pregnancy test performed on a woman, a mother's physical conditions, and other relevant status of the subject in question.

The measurements (measured results) taken in medical examination vary depending on a number of factors. These factors include the patient's pathologic conditions, physical differences among a plurality of subjects, the number of weeks of pregnancy for a pregnant woman, and other individual circumstances of the subject in question.

The conventional medical measurement apparatuses have their measuring items established in advance and do not allow the items to be modified according to individual subjects. With all measurements displayed numerically by those apparatuses, any operator with no specialized knowledge finds it difficult to make a proper judgment on the measured results.

In the conventional medical measurement apparatuses, even where criteria for judgment (i.e., cut-off values) are established, the criteria are fixed for all potential and actual patients. The comments about measurements with respect to the criteria are limited mostly to such simple statements as "high" and "low." In such a conventional setup, the subject is unable to grasp his conditions properly.

In contrast, the medical measurement apparatus 10 of the invention allows suitable items of measurement to be selected for individual subjects by the controller. Illustratively, the measuring items are selected by purpose: for determining pregnancy, grasping the mother's physical conditions, and finding the patient's pathologic conditions. Appropriate criteria for judging the measured results are also set up, and a variety of comments about the measured results with respect to the criteria are provided by the controller such as doctor. Such comments provided by the controller may include: "You are in good health," "Contact our hospital as soon as possible," "See your doctor at our hospital as soon as possible," "Take the drug," "Stop taking the drug," and "Take measurements (of another measuring item)." It is also possible to set an appointment for the next measurement or examination.

With the inventive medical measurement apparatus 10, such measuring items, criteria for judgment and comments may be set or modified as needed only by the controller such as a doctor with specialized knowledge.

Commands may be executed in place of or in addition to the comments displayed. Although the display of comments may be regarded as a kind of commands, separate commands should preferably be furnished illustratively as follows:

(1) A command may cause the apparatus to take measurements of another item X hitherto-unauthorized, triggering display of a comment "Measure X next" to prompt the operator to proceed with the measurement.

(2) Another command may cause the apparatus to transmit an alarm to the host computer of the controller, to communicate with the controller's host computer via a communication line, or to place a telephone call to the controller.

(3) On the basis of the measurements taken of the first target analyte, another command may cause the apparatus to modify the criteria for judging the second target analyte to be examined.

(4) Another command may cause the apparatus to alter the constraints on the dates on which measurement is authorized.

(5) Another command may cause the apparatus to transfer the measured results to the host computer or server on the part of the controller.

(6) Another command may cause the apparatus to call via a communication line an examination appointment status screen as well as such service programs as an examination appointment entry program from the controller's host computer or server.

(7) Another command may cause the apparatus to retrieve information from relevant data sources (e.g., database).

Execution of the above commands is desired in situations where the controller and the subject are separated over a long distance or where the measurement and the care involved are highly urgent. Where the subject or operator is not expected to seek relevant medical care promptly due to impediments such as

advanced age, the controller should preferably set in advance necessary measures as commands to ensure appropriate medical care.

According to the medical measurement apparatus of the invention, individual subjects are allowed to take measurements best fit for themselves inside or outside medical institutions, to receive experts' judgments on their measurements in an individually customized manner, and to take necessary action as prompted such as visits to the doctor or changes in the frequency of measurement. Measurement and medical treatment are thus made available effectively and efficiently to those who need them. The medical measurement apparatus allows the subjects to live with a sense of security at home or elsewhere by taking measurements on their own and verifying the experts' judgments on their measurements. The measured results provide a very effective aid to those engaged in taking care of the subjects. In short, the inventive medical measurement apparatus offers remotely provided, efficacious medical care to home-care situations.

Furthermore, the medical measurement apparatus of the invention is far superior to conventional systems or apparatuses in providing detailed and precise control over medical measurement by the controller such as a doctor and a pharmacist with specialized knowledge about medical care. The controller can make sure that the apparatus is appropriately utilized and that incorrectly acquired measurements do not result in misdiagnosis. It is also possible to inhibit the measurement of items not authorized to a specific subject and to prevent the abuse of individually acquired measurement information.

There are no specific constraints on the manner in which to set the items of measurement, the criteria for judgment, or comments. The same methods as those cited above in connection with the entry of identification data may also be employed. It is not necessary to match one measuring item with a single criterion and a single comment; each measuring item may correspond to a plurality of criteria as well as to a plurality of comments and commands. This makes it possible to provide more precise, fine-tuned medical measurement tailored to each subject.

Likewise, no specific constraints exist on the way in which the controller alone is allowed to set the criterion setting means. As in the case of the subject's identification data and of the manner of entering such ID data, various known methods may be used, including the use of the controller's identification code to make entries into a predetermined subroutine dedicated to the controller.

Below is an example of how the controller alone is permitted to set the criterion setting means.

When a subject (e.g., patient) visits the medical institution to see the controller such as a doctor for medical examination, the controller stores into a "health care card" the items of measurement appropriate to the subject's pathologic conditions, the criteria for judging measurements, comments and commands. These settings are stored by the controller using a reader-writer or a disc drive connected to the host computer, into the card in the form of a storage medium such as an IC card or a floppy disc. At the same time, the subject's name and other basic personal data on the subject are stored into the card along with a password code chosen by the subject. Entry of the data into the storage medium by the controller requires the use of the security card possessed only by the controller, the password code known only to the controller, or both.

The controller hands the health care card thus prepared over to the relevant subject, together with the security card dedicated to that subject as needed. The subject takes his health care card home and connects it to the control unit 14 of the medical measurement apparatus 10 in his possession. Upon measurement, the measured results are written to the health care card. To carry out the measuring operations requires the use of the security card possessed only by the subject, the password code known only to the subject, or both.

The control unit 14 checks to see if the intended measurement is appropriate in view of the date and time of the measurement and of the answers to preliminary questions, put to the subject. Then in accordance with the criteria set by the controller, the control unit 14 judges the measurements and displays and/or executes relevant comments and/or commands set by the controller. If the subject is unable to perform measurement on his own, an operator may take over the measuring operations from that subject.

At the time of measurement, instead of the subject selectively entering the measuring items authorized by the controller, the connected measuring unit 12 (analyzing section 12a) may alternatively discriminate and establish the appropriate measuring items automatically. The discrimination means may be any one of known means employing output signals, bar codes and a magnetic tape used for connecting the apparatus components, for shape recognition by the analyzing section 12a, and for connection with the measuring unit 12.

The judgment and display means computes measurements from electrical signals from the measuring unit 12. Comparing the measurements with the criteria, the judgment and display means selects the appropriate comment and displays it on the display unit 20.

The judgment execution means computes measurements from electrical signals from the measuring unit 12. Comparing the measurements with the criteria, the judgment execution means selects the relevant command and causes the control unit 14 to execute that command.

The illustrated medical measurement apparatus 10 of the invention preferably comprises storage means for storing and accumulating a plurality of measurements for each subject. The storage means is preferably constituted so that the controller retrieves the stored data as desired.

With the constitution above, the controller such as a doctor may reference the accumulated measurements for subsequent treatment or measurement. Because the medical measurement apparatus 10 of the invention uses its identification means to identify the subject for measurement, the resulting measurements will not be mixed up with measurements of any other subject. This allows the controller to pass an accurate judgment on the relevant measurements of the subject in question.

For the medical measurement apparatus 10 of the invention, the measurements or measured results include not only medically measured data but also the dates and time stamps of measurement, the measuring environment, measuring conditions, the subject's pathologic conditions, the subject's answers to preliminary questions put to him, the subject's reactions to the measuring conditions in effect, ambient information such as temperatures obtained by temperature sensors, and other information associated with the measurement.

The illustrated medical measurement apparatus 10 further includes questioning means for putting preliminary questions to the subject in connection with the target item to be measured, and verification means for verifying that measurement is performed under the measuring conditions established in accordance with the measuring item in effect. The questioning means and the verification means are constituted so that only the controller is authorized to set the preliminary questions as well as the measuring conditions.

The medical measurements thus taken often vary depending on the subject's conditions.

For example, measurements of urine hCG taken from trophoblastic disease vary significantly depending on the number of days that have elapsed since the subject underwent the operation. For pregnancy diagnosis, measurements of urine hCG also vary considerably depending on the number of days that have elapsed since the subject's previous menstruation period started.

Measurements of blood hPL and urine estriol taken in order to grasp the pregnant woman's condition vary quite appreciably depending on the number of weeks of her pregnancy.

Furthermore, measurements of aldosterone and plasma renin activity vary significantly depending on whether or not the subject is on an empty stomach at the time of measurement.

Meanwhile, to take measurements of stool hemoglobin requires acquiring the measurements and referring thereto every day.

To judge accurately those measurements thus requires altering or selecting the criteria for judgment (i.e., cut-off values) in accordance with the subject's condition.

The medical measurement apparatus 10 of the invention preferably puts preliminary questions to the subject with respect to the measuring items. The apparatus is constituted preferably so that, depending on the answers to the questions, the apparatus selects the criteria for judgment, comments and/or commands to be used.

For some measuring items, no measurements will be referenced and regarded as viable if the measuring conditions such as the measuring time, measuring period and temperatures are not strictly observed.

For example, measurements of aldosterone and plasma renin activity are not considered reliable if not taken early in the morning. Where instructions are to be given to the subject for taking drugs, it should be noted that measurements of the current drug concentration in blood are dependent of the time at which the subject previously took the drug. When the medication time is entered into the system in response to a preliminary question, the doctor can subsequently give appropriate instructions to the subject.

Thus the medical measurement apparatus 10 preferably includes the verification means for verifying that measurement is performed under predetermined conditions. If an attempt is made to conduct measurement under conditions other than those determined beforehand, the system will not let measurement be carried out or will give an alarm. If necessary, the system is constituted to give an alarm at a prescribed measuring time so as to prompt the subject to take measurements.

Preferably, only the controller is authorized to set the above-mentioned preliminary questions and measuring conditions.

The arrangements above permit the medical measurement apparatus to provide individual subjects with more fine-tuned and customized medical measurement.

There are no specific constraints on the manner in which to set preliminary questions or measuring conditions. The same methods as those cited above in connection with the entry of identification data may be utilized.

Similarly, there are no specific limits to the way in which only the controller is authorized to set the preliminary questions and measuring conditions.

Various known methods cited in connection with the subject's identification data and with the entry of such ID data, including the use of the controller's identification code, may be employed.

Where the preliminary questions are related to the passage of time specific to the subject (number of weeks of pregnancy, age, etc.), the data constituting the questions may be input and stored in advance in the control unit body 16. In operation, when the identification means identifies the subject, the system may automatically select the criteria for judgment or other relevant settings in keeping with the time-related conditions.

The preliminary questions may be concerned with other measurements such as blood or urine content measurements (urine sugar level, blood sugar level, etc.), blood pressure, and body temperature. With responses given to such preliminary questions, the controller can evaluate the criteria and judgments in more detail regarding individual subjects. Furthermore, the above setup makes it possible to furnish the operator (any one of nurses, clinical technicians, other doctors, etc.) with more precise, individually customized instructions that will lead to better treatment of each subject.

The inventive structures above also make it possible to avoid taking unnecessary measurements regarding the previously selected measuring items. This allows both the operator and the subject to bear less burden in medical care than before, and the resulting cost savings are considerable.

Where preliminary questions are put to the subject with respect to other measurements such as blood or urine components, blood pressure and body temperature, these measuring items may also be set in the medical measurement apparatus of this invention. The measuring unit for taking measurements regarding the preliminary questions may be either connected to or incorporated in the inventive medical measurement apparatus. In such cases, the medical measurement apparatus may be arranged to read automatically the measured results furnished in the manner described.

For example, C-reactive protein (CRP), representative of acute phase protein, measures high under such pathologic conditions as inflammatory disorders (infectious disease, appendicitis, pneumonia, hepatitis, etc.), injuries, the post-surgical stage, pregnancy and collagen disease.

For this reason, the measurement of CRP is not only an item used extensively for pathologic screening but also an item for which suitable criteria need to be set for individual subjects.

The inflammatory reaction of infectious diseases generally involves increases in body temperature. This means that the measurement of CRP is not mandatory where the body temperature remains below a certain level.

Illustratively, when the subject's temperature, given in response to a preliminary question or received from a temperature sensor, turns out to be lower than a level (e.g., 37.0°C) specific to the subject, the system may be arranged to issue a comment saying that the measurement of CRP is unnecessary.

Such an arrangement allows the measurement of CRP to be skipped where appropriate even if that measurement has been established as a measuring item. This translates into less burden on both the operator and the subject and more savings in economic terms.

The criteria for judging CRP measurements are set suitably for individual subjects. Generally the threshold value for judgment is about 200 µg/dl. for subjects 6 to 13 years old, and about 500 µg/dl. for adult subjects. The threshold value should be higher for pregnant women and patients in the post-surgical stage.

When the measurements turn out to be below the threshold value for judgment, the apparatus issues a comment saying that although there is nothing unusual at present, the subject should pay attention to subsequent changes in body temperature. If the measurements are found to be higher than the threshold value, the apparatus issues a comment prompting the subject to contact the doctor at once or executes a command calling up the doctor in charge by radio pager or the like.

Shown below are tables listing typical preliminary questions, cut-off values, comments and other related data which may be furnished in connection with measuring items.

The listings are only for illustration, and they may be altered as needed by the controller in accordance with the subject's pathologic conditions and with physical differences among individual subjects.

Table 1

Measuring Items	Preliminary Questions	Measurable Time	Cut-off Values	Alarm Set Up	Comment: Lower than Cut-off Value	Comment: Cut-off Value or Higher
Urine hCG (for pregnant women)	Select the number of weeks that elapsed since the day your previous menstruation period started.	Unrestricted		Unnecessary		
	1. More than 3 weeks and not less than 4 weeks		0.5 mIU/ml		Take measurements again next week	See your doctor at the hospital within a week
	2. More than 4 weeks and not less than 5 weeks		Lower than 0.5 mIU/ml 0.5 to lower than 20 mIU/ml Lower than the previous measurement 20 mIU/ml or higher		You are not pregnant this time Contact your doctor immediately Contact your doctor immediately See your doctor at the hospital within a week	
	3. More than 5 weeks and not less than 6 weeks		Lower than 0.5 mIU/ml 0.5 to lower than 100 mIU/ml Lower than the previous measurement 100 mIU/ml or higher		You are not pregnant this time Contact your doctor immediately Contact your doctor immediately See your doctor at the hospital within a week	
(for ectopholastic disease)	Select the number of weeks that elapsed since the day you were operated on.	Unrestricted		Unnecessary		
	1. 5 weeks after operation		1000 mIU/ml		Take the next measurements 8 weeks after operation	Contact your doctor immediately
	2. 8 weeks after operation		100 mIU/ml		Take the next measurements 20 weeks after operation	Contact your doctor immediately
	3. 20 weeks after operation		0.5 mIU/ml		Excellent recovery. See your doctor at the hospital on your next appointed date.	Contact your doctor immediately
Urine LH	Did you take measurements yesterday?	04:00 to 08:00		Unnecessary		
	1. No, I didn't.		20 mIU/ml		Take measurement again tomorrow	Ovulation is expected within 48 hours. Take measurements again tomorrow.
	2. Yes, I did.		Yesterday's Value / This Time Value Lower than 20 mIU/ml, / Lower than 20 mIU/ml Lower than 20 mIU/ml, / 20 mIU/ml or higher 20 mIU/ml or higher, / Lower than 20 mIU/ml 20 mIU/ml or higher, / 20 mIU/ml or higher		Take measurement again tomorrow Ovulation is expected within 48 hrs. Ovulation is expected within 24 hrs. Ovulation is expected within 36 hrs.	

Table 2

Measuring Items	Preliminary Questions	Measurable Time	Cut-off Values	Alarm Set Up	Comment: Lower Than Cut-off Values	Comment: Cut-off Value or Higher
Blood progesterone	Select the number of weeks of your pregnancy.	Unrestricted				
	1. 4 to 9 weeks		15 ng/ml		Take measurements again 4 weeks later	Contact your doctor immediately
	2. 10 to 15 weeks		20 ng/ml		Normal progress. See your doctor at the hospital on your next appointed date.	Contact your doctor immediately
Stool hemoglobin	Did you take measurement yesterday?	Unrestricted				
	1. No, I didn't.		50 ng/ml		Take measurements again tomorrow	
	2. Yes, I did.		Yesterday's Value: Lower than 50 ng/ml; This Time Value: Lower than 50 ng/ml		Normal. Take measurements again 6 months later	
			Yesterday's Value: Lower than 50 ng/ml; This Time Value: 50 ng/ml or higher		Take measurements again tomorrow	
			Yesterday's Value: 50 ng/ml or higher; This Time Value: Lower than 50 ng/ml		Take measurements again tomorrow	
			Yesterday's Value: 50 ng/ml or higher; This Time Value: 50 ng/ml or higher		See your doctor at the hospital within a week	
	3. Yes, yesterday and the day before yesterday.		50 ng/ml		Normal. Take measurements again 3 months later	See your doctor at the hospital within a week

Table 3

Measuring Items	Preliminary Questions	Measurable Time	Cut-off Values	Alarm Set Up	Comment	
					Lower Than Cut-off Values	Cut-off Value or Higher
Blood HPL	Select the number of weeks of your pregnancy. 1. 6 to 9 weeks 2. 10 to 13 weeks 3. 14 to 18 weeks	Unrestricted	 0.01 μg/mL 0.16 μg/mL 0.64 μg/mL	Unnecessary	Contact your doctor immediately	Take measurements again next week
Omina estriol	Select the number of weeks of your pregnancy. 1. 32 to 36 weeks 2. 37 to 38 weeks 3. 39 to 41 weeks	Unrestricted	 5 ng/L 10 ng/L 25 ng/L	Unnecessary	Contact your doctor immediately	Take measurements again next week
Aldosterone	Are you taking this measurement after at least 30 minutes of rest on an empty stomach? YES NO	04:00 to 08:00	 130 ng/mL 210 ng/mL	Necessary	Normal	Contact your doctor immediately
Plasma renin activity	Are you taking this measurement after at least 30 minutes of rest on an empty stomach? YES NO	04:00 to 08:00	 4.4 ng/mL 10.5 ng/mL	Necessary	Normal	Contact your doctor immediately
ASO	Select the subject's age bracket. 1. Preschool child 2. School child 3. Adult	Unrestricted	 250 U 330 U 250 U	Unnecessary	Normal value, though, take measurements again next week to make sure	Contact your doctor immediately

Table 4

Measuring Items	Preliminary Questions	Measurable Time	Cut-off Values	Alarm Set Up	Comment: Lower than Cut-off Value	Comment: Cut-off Value or Higher
Blood CEA	Your scheduled day of measurement is December 10, 1993.	Unrestricted	5 ng/ml	Unnecessary	Normal value. Take measurements again on the next scheduled day, January 10.	See your doctor at the hospital within a week.
	When try to take measurements before the scheduled day of measurement				The system displays a comment saying "today is not your scheduled day of measurement yet. Wait until December 10." The system is not operable for measurement.	
	When try to take measurements after the scheduled day of measurement				The system displays a comment saying "although today is past your scheduled day of measurement, you can proceed with measurement now. Try to be on time next time." The system is for measurement.	
Blood AFP	Your scheduled day of measurement is December 10, 1993.	Unrestricted	20ng/ml	Unnecessary	Normal value. Take measurements again on the next scheduled day, January 10.	See your doctor at the hospital within a week.
	When try to take measurements before the scheduled day of measurement	Unrestricted			The system displays a comment saying "today is not your scheduled day of measurement yet. Wait until December 10." The system is not operable for measurement.	
	When try to take measurements after the scheduled day of measurement				The system displays a comment saying "although today is past your scheduled day of measurement, you can proceed with measurement now. Try to be on time next time." The system is for measurement.	

As mentioned above, the medical measurement apparatus of the invention allows the controller to alter as needed the criteria for judgment, comments, and preliminary questions depending on the subject's pathologic conditions and on physical differences among subjects.

For example, as shown in Table 4 above, the cut-off value of blood CEA measurements is usually 5 ng/ml. However, if the mean value ± standard deviation of blood CEA measurements over a certain past

period was 3.0 ± 1.0 ng/ml, the controller may alter the cut-off value to 4 ng/ml. This ensures more accurate measurement.

In the example of Table 1 above, the urine LH concentration is allowed to be measured between 4:00 and 8:00 a.m., and the criteria for judgment (cut-off values) center on 20 mIU/ml.

It may happen that the urine LH concentration measurements over the past three months have indicated that the urine LH concentration during ovulation of a particular subject who wants to become pregnant is lower than that of the average woman (20 mIU/ml or higher). With the default settings in effect, it is difficult for the subject in question to find the peak urine LH concentration during ovulation. In that case, the measurable time may be set alternatively for 4:00 to 8:00 as well as for 16:00 to 20:00, the cut-off values may be supplemented with a value of 10 mIU/ml, and the comments may be modified as shown below. These modifications allow the subject to find more precisely the peak urine LH concentration during ovulation.

Preliminary Questions

1. Is this your first measurement?
2. Is this your second or subsequent measurement?

Cut-off Values and Comments

If your answer to preliminary question 1 is "YES":
(Cut-off values): Lower than 10 mIU/ml
(Comment): Take measurements again 12 hours later.
(Cut-off values): 10 mIU/ml or higher, lower than 20 mIU/ml
(Comment): Ovulation is expected within 48 hours. Take measurements again 12 hours later.
(Cut-off values): 20 mIU/ml or higher
(Comment): Ovulation is expected within 24 hours.

If your answer to preliminary question 2 is "YES":
(Cut-off values): 20 mIU/ml or higher
(Comment): Ovulation is expected within 24 hours.
(Cut-off values): Lower than 10 mIU/ml both last time and this time
(Comment): Take measurements again 12 hours later.
(Cut-off values): Lower than 10 mIU/ml last time, 10 mIU/ml or higher and lower than 20 mIU/ml this time
(Comment): Ovulation is expected within 48 hours.
(Cut-off values): 10 mIU/ml or higher last time, equal to or lower than previous measurement this time
(Comment): Ovulation is expected within 24 hours.
(Cut-off values): 10 mIU/ml or higher last time, equal to or higher than previous measurement and lower than 20 mIU/ml this time
(Comment): Ovulation is expected within 36 hours.

Regarding the urine hCG measurements for patients with trophoblastic disease shown in Table 1 above, the criteria for judgment and the comments are set in accordance with the number of weeks that elapsed since the day the subject was operated on. It may happen that when the patient with trophoblastic disease is apparently in remission, urine hCG measurements are desired to be taken to make sure that the patient has not relapsed. In that case, the preliminary questions, measurable time, cut-off values and comments in Table 1 may be modified as follows:

Measurable Time
4:00 to 8:00 a.m.

Preliminary Questions

1. Is this your first measurement?
2. Is this your second or subsequent measurement?

Cut-off Values and Comments
If your answer to preliminary question 1 is "YES":
(Cut-off values): Lower than 1 mIU/ml

(Comment): Take measurements again 2 week later.
(Out-off values): 1 mIU/ml or higher
(Comment): See your doctor at our hospital within a week.
If your answer to preliminary question 2 is "YES":
(Out-off values): Lower than 0.5 mIU/ml last time, less than 5 mIU/ml this time
(Comment): Take measurements again 4 weeks later.
(Out-off values): Lower than 0.5 mIU/ml last time, 0.5 mIU/ml or higher this time
(Comment): See your doctor at the hospital within a week.
(Out-off values): 0.5 mIU/ml or higher last time, lower then previous measurement this time
(Comment): Take measurements again 4 weeks later.
(Out-off values): Equal to or higher than 0.5 mIU/ml last time, equal to or higher than previous measurement this time
(Comment): See your doctor at our hospital within a week.

How the medical measurement apparatus 10 of the invention is illustratively operated will now be described with reference to the flowcharts of Fig. 6 (controller's operations) and Fig. 7 (operator's operations).

Initially, the controller such as a doctor with specialized knowledge sets up the medical measurement apparatus 10 by inputting thereto various measurement-related requirements such as measuring items and criteria for judgment for individual subjects.

In the example of Fig. 6, the controller first enters an identification signal such as his password number to get the apparatus ready for entry of the measurement requirements. Then with each particular subject in mind, the controller enters into the apparatus the subject's name (patient's name), the subject's ID code, an item or items of measurement, criteria (out-off values) for judging measurements regarding the specified measuring item(s), comments to be issued when the measured results are above or below the out-off values, the date for starting measurement, the date for ending measurement, a permitted period for measurement, and the execution or nonexecution of a measuring time alarm, etc.

If the controller does not enter specific values or comments for any measuring item, the apparatus automatically establishes preset data by default.

These settings and entries are made by use of the keyboard 18 attached to the control unit 14. All data entered through the keyboard 18 is displayed on the display unit 22 for verification (this also applies when the patient operates the apparatus, as will be described later).

As already described, these settings and entries may be recalled and altered as needed by the controller.

Each of the entries is stored into the corresponding memory in the control unit body 16. For example, the patient's name and the patient's ID code are stored into the memory for the identification means; the measuring items, out-off values and comments are stored into the memory for the criterion setting means; and the times for starting measurement are stored into the memory for the verification means.

When the medical measurement apparatus 10 is set up in the above manner, the apparatus is ready for use by the patient.

When the medical measurement apparatus 10 starts to be used, an alarm marking the time for starting measurement is activated if the controller has set the apparatus for alarm activation. With the alarm activated, the apparatus enters a start-up state.

In the start-up state, the patient (subject and operator) enters his name, his ID code and the relevant measuring items. When a given item is entered, the control unit body 16 retrieves the item from the corresponding memory for display and verification.

If any entered item is not correct, an alarm beep is sounded and the start-up state is reached again.

When the entered item is correct, the patient's past measured results of this item are displayed on the display unit 22.

The date of measurement is verified next. If the entered date is not correct, the alarm beep is sounded and the start-up state is reached again.

When the entered date of measurement is correct, the display unit 22 gives a comment saying that the date is correct. A specimen is then supplied to the measuring unit 12 and measurement is started.

The output signals (electrical signals) from the measuring unit 12 are sent to the judgment and display means of the control unit body 16.

The judgment and display means, for its part, computes measured results from the received output signals, selects the relevant comment based on the measured results and according to the criteria for judgment, and displays the comment on the display unit 22. At the same time, the date of measurement, the measured results and the other related data are stored into the storage means.

Alternative ways to operate the medical measurement apparatus 10 of the invention will now be described with reference to the flowcharts of Fig. 8 (controller's operations) and Fig. 9 (operator's operations). These examples are ones in which preliminary questions are put to the person operating the apparatus and the apparatus proceeds with measurement in accordance with the answers given in reply to these questions.

The examples in Figs. 8 and 9 are primarily the same as those of Figs. 6 and 7 except that the preliminary questions are asked. The description that follows will center on the differences between the two groups of examples (the same will also apply to examples of Figs. 10 through 13 to be explained later).

The controller, as in the earlier examples, first enters the patient's ID code or other appropriate identification data, as well as preliminary questions and comments about possible answers to the preliminary questions (judgments). Later, the operator enters the measuring item(s) and the patient's ID code to check if the entered item is correct. In this example, the input of the patient's name is replaced by that of the patient's ID code and is thus omitted. Then a check is made to see if there are any preliminary questions that have been set. If such questions exist, they are displayed on the display unit 22. The operator enters answers to the preliminary questions, and proceeds with measurement by following predetermined procedures or in accordance with the instructions from the apparatus, as shown in the flowchart.

Other alternative ways to operate the medical measurement apparatus 10 of the invention will now be described with reference to the flowcharts of Fig. 10 (controller's operations) and Fig. 11 (operator's operations). These examples are ones in which the settings of measurable dates and times vary with the measuring items.

The controller unlocks the hardware (i.e., control unit body 18) using the password number or ID code, and enters the patient's ID code, the measurable items, measurement starting date, and other appropriate settings. In this example, the setting of the patient's name is replaced with the patient's ID code and is omitted. Then a check is automatically made to see if each measuring item is correct. The manner of conducting the check is the same as that discussed above in connection with attaching the measuring chip (i.e., analyzing section 12a or output section 12b) to the medical measurement apparatus 10. The comment to be displayed in any measuring item is stored in advance.

The operator connects the measuring chip to the system and enters the patient's ID code. The system then verifies the patient's ID code, the measuring items (automatically checked by the measuring chip as mentioned), and the date and time of measurement, and passes judgments thereon. Where necessary, the display unit 22 displays comments relevant to these judgments. When all measuring conditions are found to match the set conditions, the operator proceeds with measurement by following predetermined procedures or according to the instructions given by the apparatus.

Further alternative ways to operate the medical measurement apparatus 10 of the invention will now be described with reference to the flowcharts of Fig. 12 (controller's operations) and Fig. 13 (operator's operations). These examples are ones in which the medical measurement apparatus 10 is connected to the host computer 100 on the controller's side and in which the cut-off values for judging measured results are replaced by numerical operation expressions for cut-off purposes. The measured results are judged based on the computed values, and comments are displayed accordingly.

The controller unlocks the software of the host computer using the password number or ID code. If there exists data representing past measurements, the controller may examine that data. The controller then specifies either new entry or entry modification. If any of the stored settings need to be modified in accordance with the result of examination of the patient's data, the controller alters the relevant measuring items, cut-off numerical operation expressions and other settings. For the new entry of settings, the controller inputs a new patient's name, measuring items and other data. The controller then locks the software.

The operator connects the measuring chip to the apparatus and enters the patient's ID code. This causes the apparatus to verify the patient's ID code, the measuring items (automatically checked by the measuring chip), date and time of measurement, and other settings. Comments relevant to the judgments by the apparatus are displayed on the display unit 22. When all conditions are found to match the set conditions, the operator proceeds with measurement by following predetermined procedures or according to the instructions provided by the apparatus.

Other alternative ways to operate the medical measurement apparatus 10 of the invention will now be described with reference to typical displays on the display unit 22 shown in Fig. 14 (a control panel in effect when the controller starts entering settings), Fig. 15 (a control panel in effect when the controller enters measurement-related settings), Fig. 16 (a control panel in effect when the operator starts measurement), and Fig. 17 (a control panel showing the controller's comment when the operator ends measurement). The

medical measurement apparatus 10 shown illustratively herein has an LCD acting as a control panel on the display unit 22 (Fig. 1). The keyboard may be used to enter characters into the fields and the mouse may be operated to manipulate push virtual buttons on the displayed control panel.

When the controller starts an entry procedure by activating a group of subject entry commands, the display unit 22 displays the control panel of Fig. 14 requesting the input of the controller's password code. When the controller's password code is entered through the keyboard and the "OK?" button is clicked with the mouse, the control unit compares the input code with the stored password code. If the input code is found to coincide with the stored password code, the display unit 22 displays the control panel of Fig. 15 for the entry of settings. If the input code and the stored password code fail to coincide with each other, the start-up state is reached again and another input of the controller's password code is requested.

The control panel of Fig. 15 comprises a subject (patient) name input field, a subject ID (password) code input field, a ring switch for selecting the target analyte to be analyzed, an entry date indication field, an entry time indication field, a criterion (cut-off) setting slide switch, a comment input field for giving a comment when the measured result is equal to or higher than the criterion, a comment input field for giving a comment when the measured result is lower than the applicable criterion, a ring switch for setting date to permit start of measurement (day, month, year), a ring switch for setting date to permit the end of measurement (day, month, year), a ring switch for setting a day of the week on which to permit measurement, a ring switch for setting a measurable time range, an alarm setting push button, an entry verification push button, and an input field in which to enter the controller's password code at the time of data entry.

In the example of Fig. 15, a patient named "T. Yamauchi" is entered with a code name "OHU1." The target analyte to be analyzed is set for "urine hCG" and the criterion for measured result is set for "50 IU/L." When the measured result exceeds the established criterion, the control panel is set to display a comment saying, "Congratulations. You are probably pregnant. Contact your doctor as soon as possible at the M hospital (call 03-XXXX-XXXX)." When the measured result is lower than the applicable criterion, the control panel is set to display a comment saying, "You are probably not pregnant. If you are in doubt, contact your doctor any time at the M hospital (call 03-XXXX-XXXX)." The date on which measurement is allowed to start is set for "Now." The date on which measurement is allowed to end is set for "October 31 this year." The day of the week on which to conduct measurement is not restricted, whereas the measurable time range is limited to the early morning between 4:00 and 8:00. The alarm is turned off. When these settings are entered and considered satisfactory, the controller enters his password code and pushes the "entry verification push button." This causes the control unit 14 to store the settings into the storage means.

The operator, for her part, operates the control unit 14 on the basis of the settings entered by the controller. The control panel of Fig. 16, in effect when the control unit 14 starts measurement, presupposes that the operator and the subject are the same person. That is, when the control unit 14 starts measurement, the display unit 22 displays the control panel of Fig. 16. This control panel comprises a ring switch for selecting the subject name, a subject password code input field, a measurement date indication field, a measurement time indication field, a ring switch for selecting the target analyte to be analyzed, a measured result indication field, a graphic indicator for showing measured results, a comment indication field ("Remarks" field), a graphic indicator for showing her past data, a ring switch for determining whether or not to save measured results, and a push button for deciding whether or not to perform the next measurement continuously.

The operator cannot start measurement unless he selects the patient's name, enters the correct subject ID code, and chooses the target analyte allowed for measurement. Furthermore, the intended measurement cannot be started if it does not fall on the date of measurement authorized by the controller or within the permitted time range for measurement. When the entries made by the operator are correct and satisfy the conditions set by the controller, the graphic indicator for showing past data displays the subject's past measurement data in the form of a simple line chart, with the "Remarks" field giving a message prompting the operator to start measurement. If the intended measurement is not permitted for some reason, that reason is displayed in the "Remarks" field and the control unit returns to the start-up state. When measurement is permitted, the operator gets the hCG analyzing section (shown in Figs. 3 and 4) placed into the measuring unit (because "urine hCG" is selected as the target analyte to be analyzed for this example), introduces a urine specimen into the analyzing section, and starts measurement. The measured result is displayed five minutes later, and the "Remarks" field displays a controller-set relevant comment in accordance with the criteria set by the controller.

When measurement is ended, the display unit 22 displays the control panel of Fig. 17. In this example, the measurement taken is 200 IU/L, a value exceeding the applicable criterion. The control panel thus

displays a comment set by the controller in advance saying, "Congratulations. You are probably pregnant. Contact your doctor at the M hospital (call 03-XXXX-XXXX) as soon as possible."

Typical operating procedures of the medical measurement apparatus 10 of the invention as well as the internal workings of the control unit 14 will now be described with reference to Figs. 18 (on the controller's side) and Fig. 19 (on the operator's side). The operations in Fig. 18 correspond to the flowchart of Fig. 6 as well as to the control panels (displayed on the display unit 22) of Figs. 14 and 15, and the operations in Fig. 19 correspond to the flowchart of Fig. 7 as well as to the control panels of Figs. 16 and 17.

When the controller starts an entry procedure by activating a group of subject entry commands, the control unit 14 (or host computer) enters an operation mode shown in Fig. 18. The controller ID code entered through the keyboard is compared by a comparator 110 with the controller registration code stored in the storage means. In case of a match (a "true" output from the comparator), an AND gate 1 and an AND gate 2 are opened. The conditions entered and set from the keyboard 18 and from the push button switches and slide switches on the control panel are sent past the AND gate 1 for temporary storage into memory (RAM). When the "ENTER?" push button is clicked, the output of the AND gate 2 becomes "true" so as to open an AND gate 3. The settings in the temporary memory are then written to the applicable regions in the storage means.

Meanwhile, when the operator starts a group of measuring commands, the control unit or host computer enters a measurement mode shown in Fig. 19. In the measurement mode, the output of current time data from a built-in timer in the control unit 14 is compared by a comparator 112 with the settings of measurement date and time data stored in the storage means. If the output of the current time data from the timer falls on the allowed date and within the allowed time period, the comparator 112 outputs a "True" signal to open the AND gate 1 and an AND gate 3. Where the controller set alarm activation beforehand in the storage means, the opening of the AND gate 3 turns on a buzzer or other appropriate type of alarm. When the subject name is selected by use of a ring switch on the control panel of the control unit 14, the opening of the AND gate 1 is accompanied by the retrieval from the storage means of the patient's name, the patient's ID code and the relevant measuring items in accordance with the ring switch for the selected subject's name. The patient's ID code thus called up is compared by a comparator 114 with the subject's ID code entered from the keyboard. If the two codes coincide with each other (a "true" output from the comparator), the AND gate 2 is opened. With the AND gate 2 opened, the measuring item selected by a ring switch and the previously recalled measuring item are compared by a comparator 116. If the comparator 116 effects a "true" output, the output enables a switch that causes the installed measuring unit 12 to start measurement. This in turn triggers the retrieval from the storage means of the criterion (cut-off value) C and the comment in effect when the measured result taken is lower than, equal to, or more than the cut-off value in accordance with the ring switch for the selected target analyte to be analyzed.

Although not shown in Fig. 19, past measured results are retrieved if the comparator 116 effects the "True" output. The output of the comparator 116 opens the AND gate through which the past data is displayed on the control panel.

When the operator installs the measuring unit 12, introduces a specimen into the measuring unit 12 (i.e., analyzing section 12a), and turns on the measurement start switch (indicated by numeral 122 in Fig. 19). This causes the measuring unit 12 to start measurement. The measured result of the target analyte is computed from the electrical signals supplied by the measuring unit 12. The value X is compared with the cut-off value C by comparators 118 and 120. Depending on whether $X \geq C$ or $X < C$, either an AND gate 4 or an AND gate 5 is opened. Then the relevant comment set by the controller is sent through an OR gate 2 for display onto the control panel. The measured result of the target analyte for analysis is stored into the storage means past an OR gate 1 along with such data as the patient's ID code, the measuring items and the measurable time.

In the examples discussed above, not all items need to be stored into a single storage means. The items may be stored in a distributed manner in a plurality of storage means. Alternatively, the same data may be stored in duplicate fashion in a plurality of storage means. The alternative way of storing the same data in a plurality of storage means is desirable from the standpoint of data security. The storage means may or may not be attached fixedly to the control unit. The storage means may be allocated in the host computer connected via communication lines, or may be of a type detachable from the control unit such as an IC card, as discussed earlier.

When the controller sets commands with respect to the measurements taken according to the criteria, such commands may be formed in files as command groups and stored in the storage means. The command groups, written in a language executable by the CPU of the control unit, may include programs written in machine language, in macro control commands such as assembler, or in higher level languages such as C, FORTRAN and BASIC. It may be desired that the CPU control devices built in or externally

attached to the control unit. Such devices may comprise the measuring unit, storage unit, alarm, communication interface, modem, facsimile machine, data I/O interface and relay circuit. In those cases, the above-mentioned command groups are supplemented by other groups of commands that are specific to the respective devices. For example, some devices are controlled by use of commands associated with the RS-232C port, parallel port or GPIB bus. Various commands may be used depending on the nature of what needs to be controlled and on the type of device to be controlled. Illustratively, there are commands that are used to modify the preliminary questions, measuring items, criteria for judgment, the comments and commands about the measured results according to the criteria, and the measurable date and time. These groups of commands are furnished initially to designate in the applicable storage unit the address of the settings desired to be modified so that they may be updated. For example, if a particular setting of the criteria exists at a specific logical address on the hard disc in the control unit, that logical address may be designated as a parameter 1, and commands for writing a parameter 2 (new setting) are preserved in the form of a preset command file. Although such command groups may be set originally by the controller, it is preferable to prepare beforehand a plurality of groups of frequently used commands as files inside the system so that the controller may simply designate the appropriate file name and parameters when setting up the commands. In the setup above, preparing commands for modifying a setting of the criteria requires three things: specifying a preset command file (comprising storage update commands), setting the parameter 1 to designate modification of the criteria, and setting the parameter 2 to designate the new setting of the criteria. As in the case of the comment display described earlier, a comparator compares the cut-off value C with the measured result X about the target analyte for analysis, the value X being computed from the electrical signals sent by the measuring unit. The corresponding command file to be set by the controller is retrieved from the storage means and executed. As described, the simplest and the least error-plagued method for the controller to set command groups is first to store all commands beforehand in the storage means, and then to select any of them in the form of a command file at the time of the controller's registration of the subject into the apparatus. In this case, selecting a plurality of files causes the command groups in the selected files to be executed, provided the measured results satisfy the criteria. The command execution means outlined above is only an example and may be replaced by any other means by which the control unit may execute commands.

While a preferred embodiment of the invention has been described using specific terms, such description is for illustrative purposes only, and it is to be understood that changes and variations may be made without departing from the spirit and scope of the claims that follow.

EXPLOITATION IN INDUSTRY

As described, the medical measurement apparatus according to the invention allows not only health-care professionals such as doctors but also test subjects such as patients and pregnant women as well as their attendants to readily perform medical measurement in medical institutions or elsewhere (e.g., at home). Furthermore, the inventive medical measurement apparatus permits health-care experts such as doctors with specialized knowledge to set appropriate comments about a given subject with respect to relevant measuring items, the criteria for judgment and the measured results. The judgments as per the criteria regarding the measured results and the relevant comments corresponding to such judgments are output suitably by the apparatus.

With this medical measurement apparatus in use, the subject staying at home can receive specialized medical care, reassured knowing that he or she is under specialists' supervision. In addition, the use of the measurements taken by this apparatus significantly helps doctors and other medical care experts in providing appropriate medical care to their patients.

Claims

1. A medical measurement apparatus comprising:

a measuring unit for outputting electrical signals in accordance with the amount of a target analyte measured in a specimen; and

a control unit including:

identification means for receiving identification data specific to a subject and for identifying said subject on the basis of said identification data;

criterion setting means only for use by a controller who sets comments about measured results regarding the measuring items and the criteria set for said subject and who is capable of making a specialized judgment on the amount of said target analyte in said specimen; and

judgment and display means for computing the measured results based on said electrical signals from said measuring unit and for selectively displaying the comment relevant to said criteria with respect to the computed measured results.

2. A medical measurement apparatus according to claim 1, wherein said identification data is set only by said controller.

3. A medical measurement apparatus according to claim 1 or 2, wherein said control unit includes storage means for storing a plurality of measured results, and wherein said controller retrieves the stored measured results as desired.

4. A medical measurement apparatus according to claim 3, wherein said storage means stores the measured results with respect to which said criteria are modified as needed.

5. A medical measurement apparatus according to any one of claims 1 to 4, wherein said control unit includes either or both of questioning means and verification means, said questioning means being used to put preliminary questions to said subject in connection with said measuring items, said verification means being utilized to verify that measurement is performed under the measuring conditions established in accordance with said measuring items, and wherein only said controller is allowed to set said preliminary questions and said measuring conditions.

6. A medical measurement apparatus according to any one of claims 1 to 5, wherein said control unit includes time stamp setting means for setting timer-counted time stamps to measure in keeping with said measuring items, and time stamp verification means for verifying that a given measurement was taken at the correspondingly set time of day, and wherein only said controller is allowed to set said time stamps.

7. A medical measurement apparatus according to any one of claims 1 to 6, wherein said criterion setting means in said control unit is arranged to set commands either in place of or in conjunction with said comments, and wherein said judgment and display means is either replaced with or supplemented by judgment execution means for selectively executing said commands.

FIG. 1

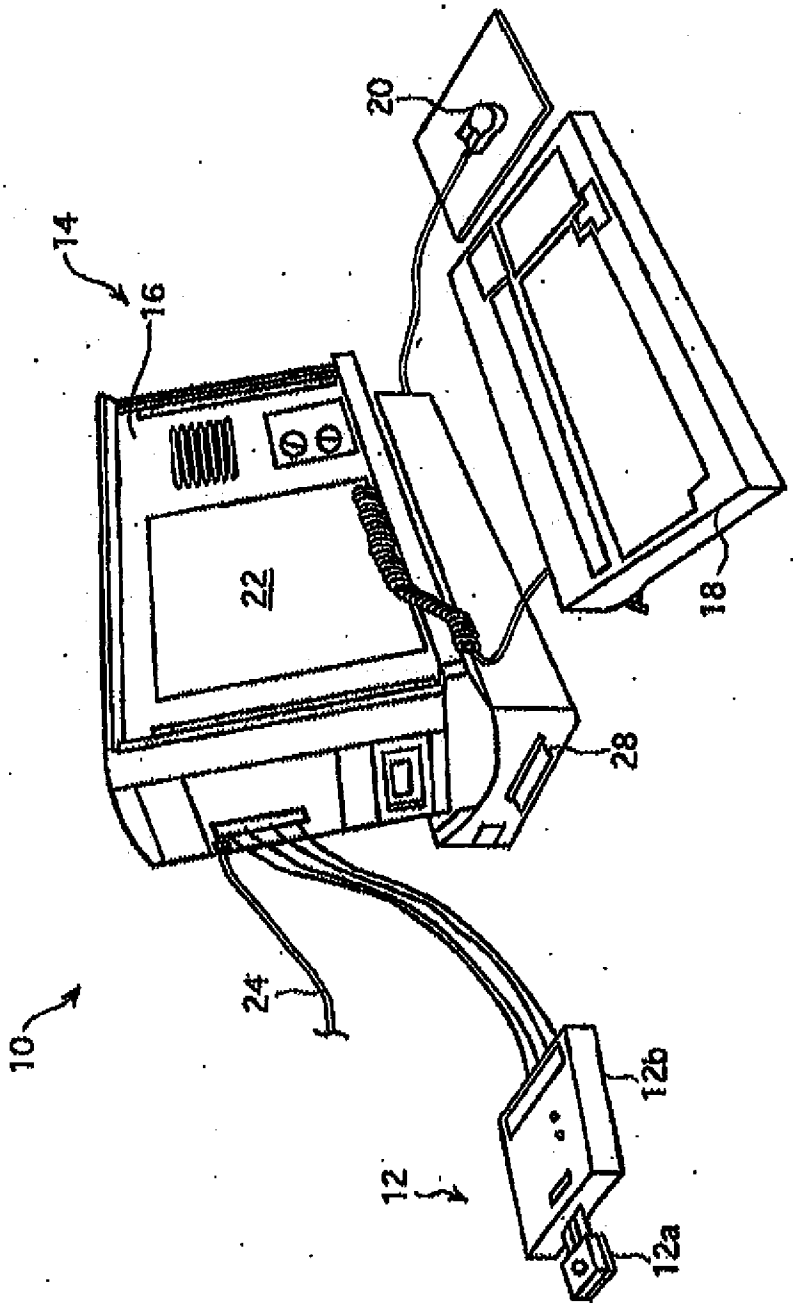


FIG.2

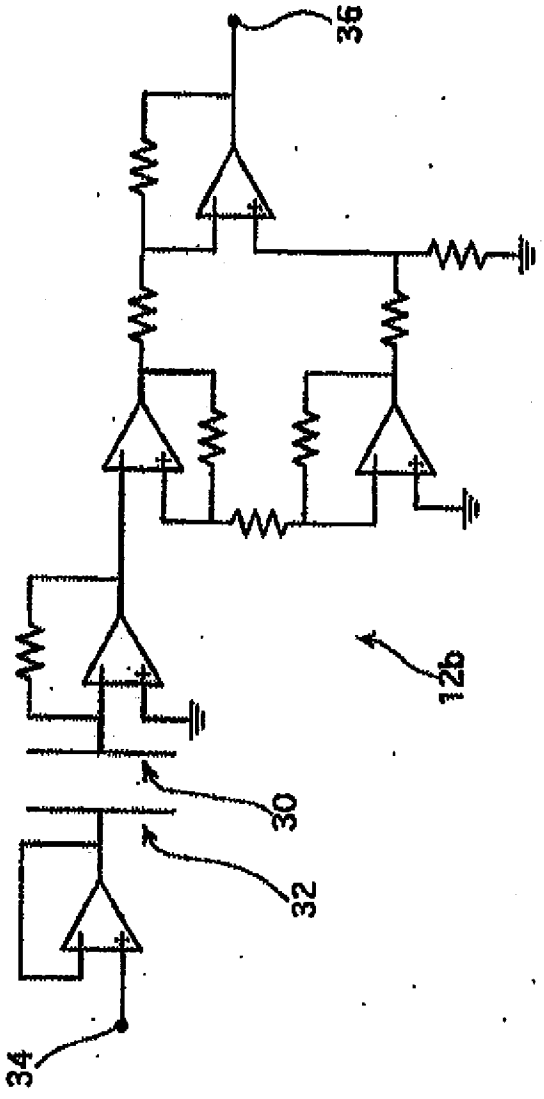


FIG.3

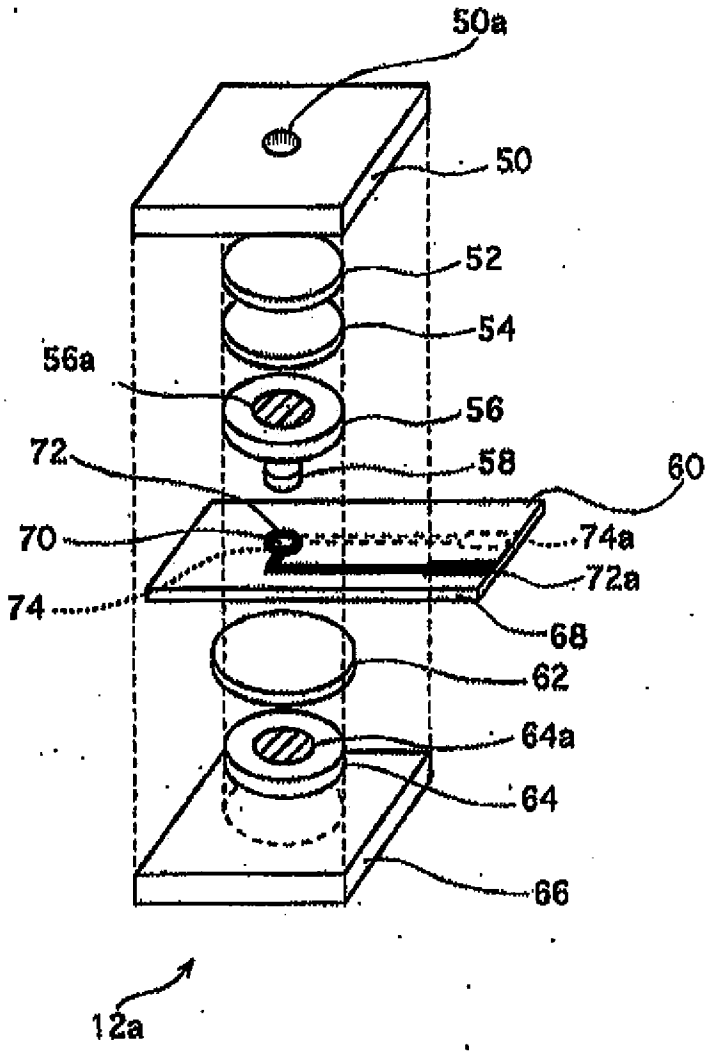
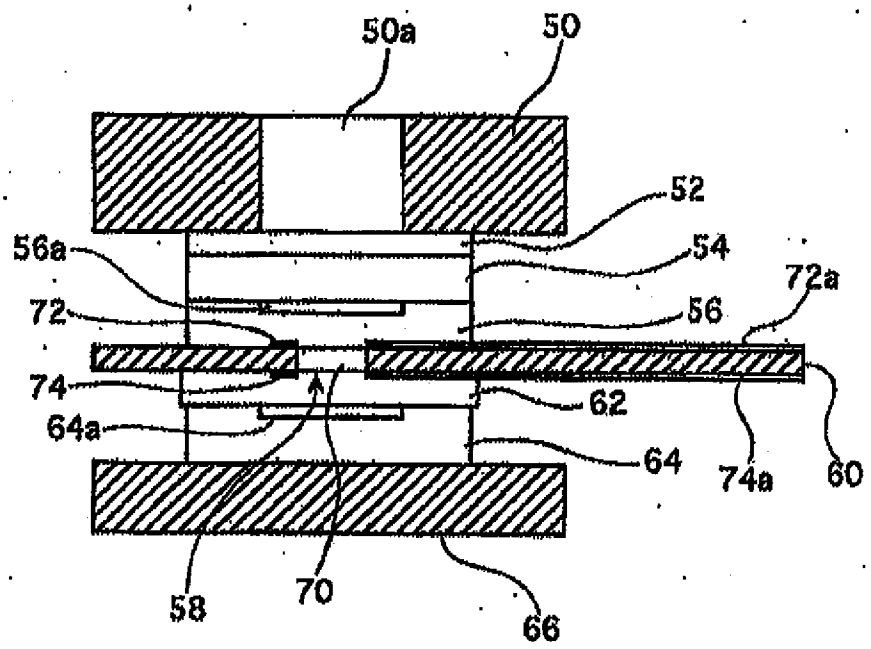


FIG. 4



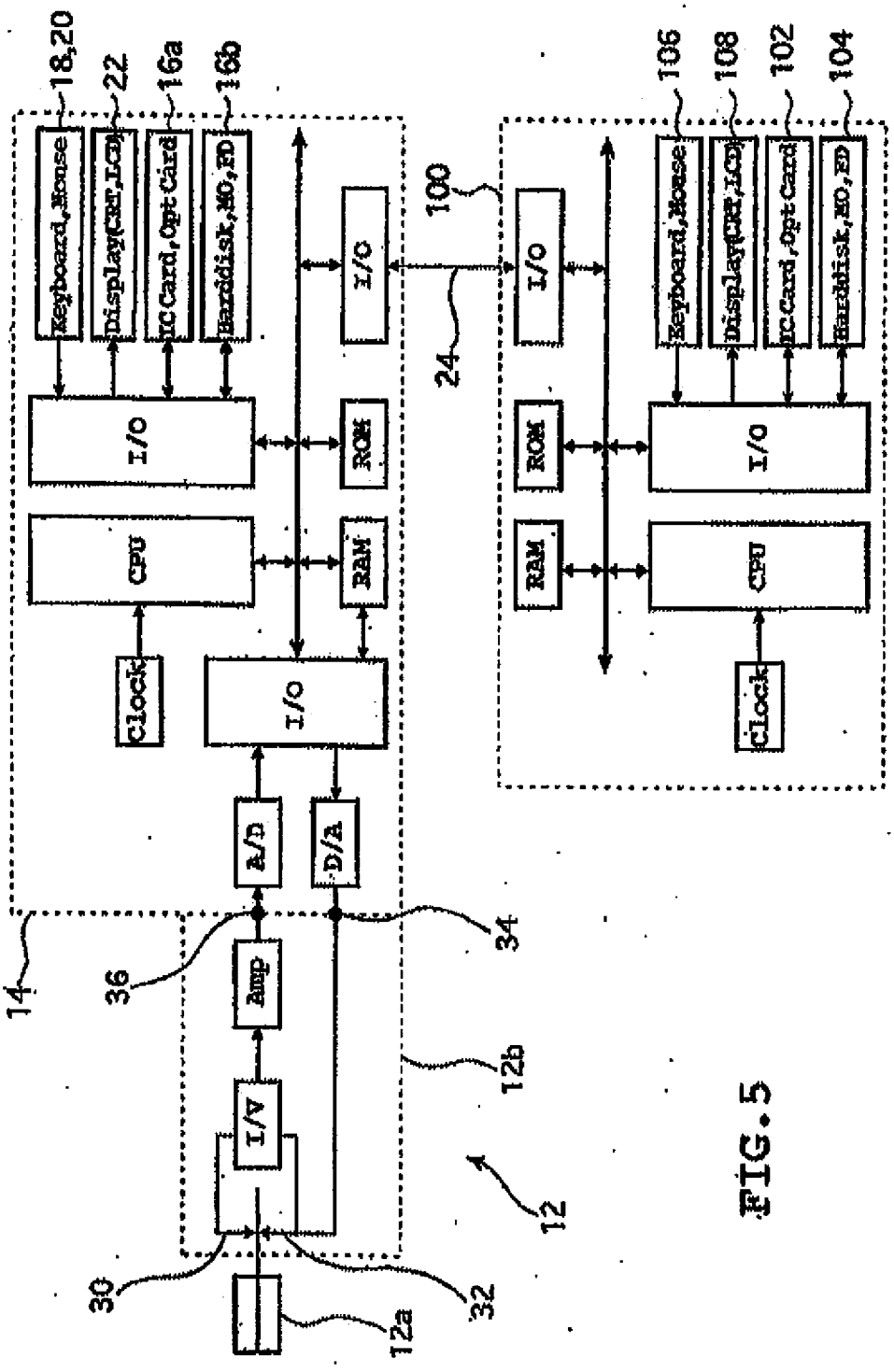

18,20
22
16a
16b
106
108
102
104
Keyboard,Mouse
Display(CRT,LCD)
IC Card,Opt Card
Harddisk,MO,FD
I/O
ROM
CPU
RAM
Clock
100
24
A/D
D/A
Amp
I/V
14
36
34
12b
12
30
32
12a

FIG.5

FIG. 6

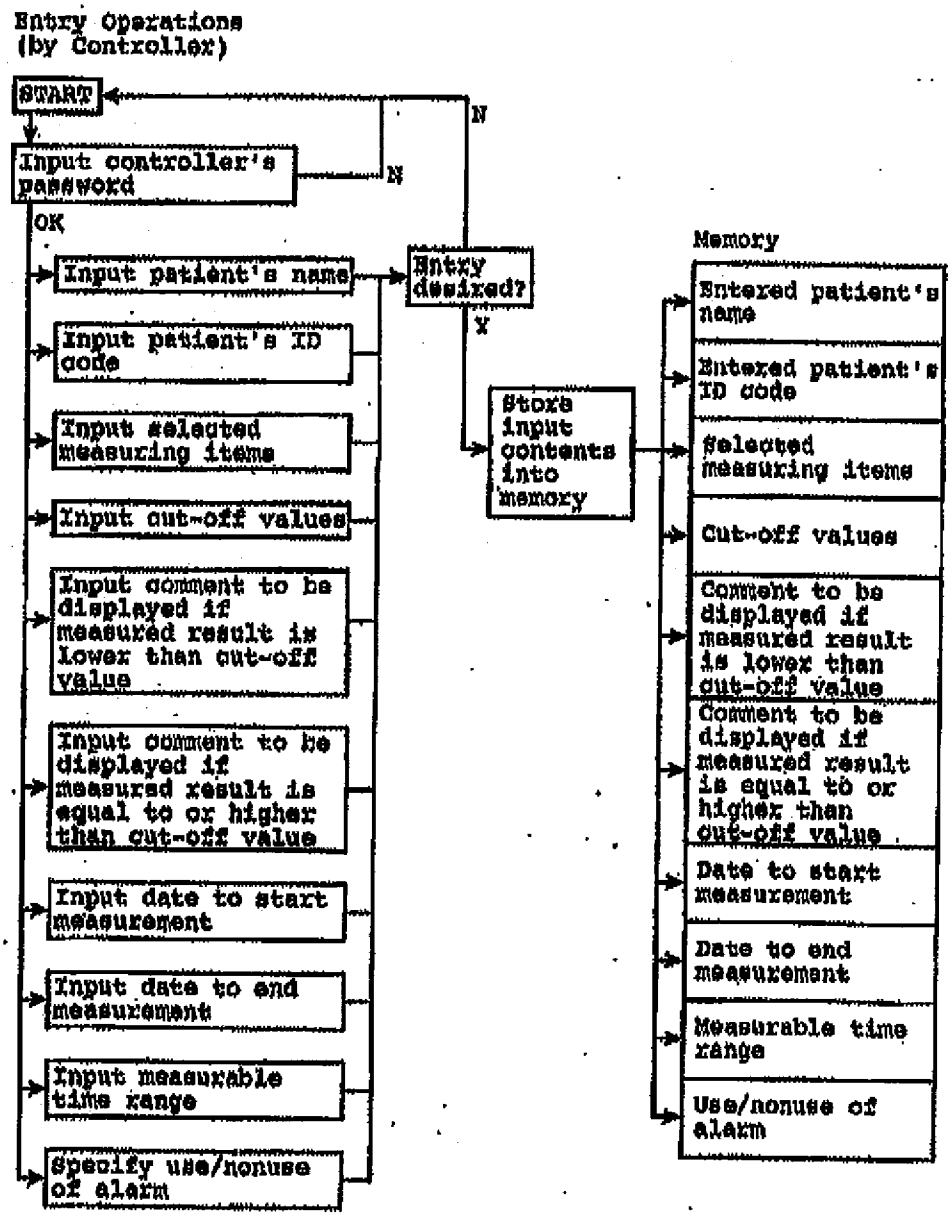

Entry Operations
(by Controller)
START
Input controller's password
N
N
OK
Input patient's name
Input patient's ID code
Input selected measuring items
Input cut-off values
Input comment to be displayed if measured result is lower than cut-off value
Input comment to be displayed if measured result is equal to or higher than cut-off value
Input date to start measurement
Input date to end measurement
Input measurable time range
Specify use/nonuse of alarm
Entry desired?
Y
Store input contents into memory
Memory
Entered patient's name
Entered patient's ID code
Selected measuring items
Cut-off values
Comment to be displayed if measured result is lower than cut-off value
Comment to be displayed if measured result is equal to or higher than cut-off value
Date to start measurement
Date to end measurement
Measurable time range
Use/nonuse of alarm

FIG. 7

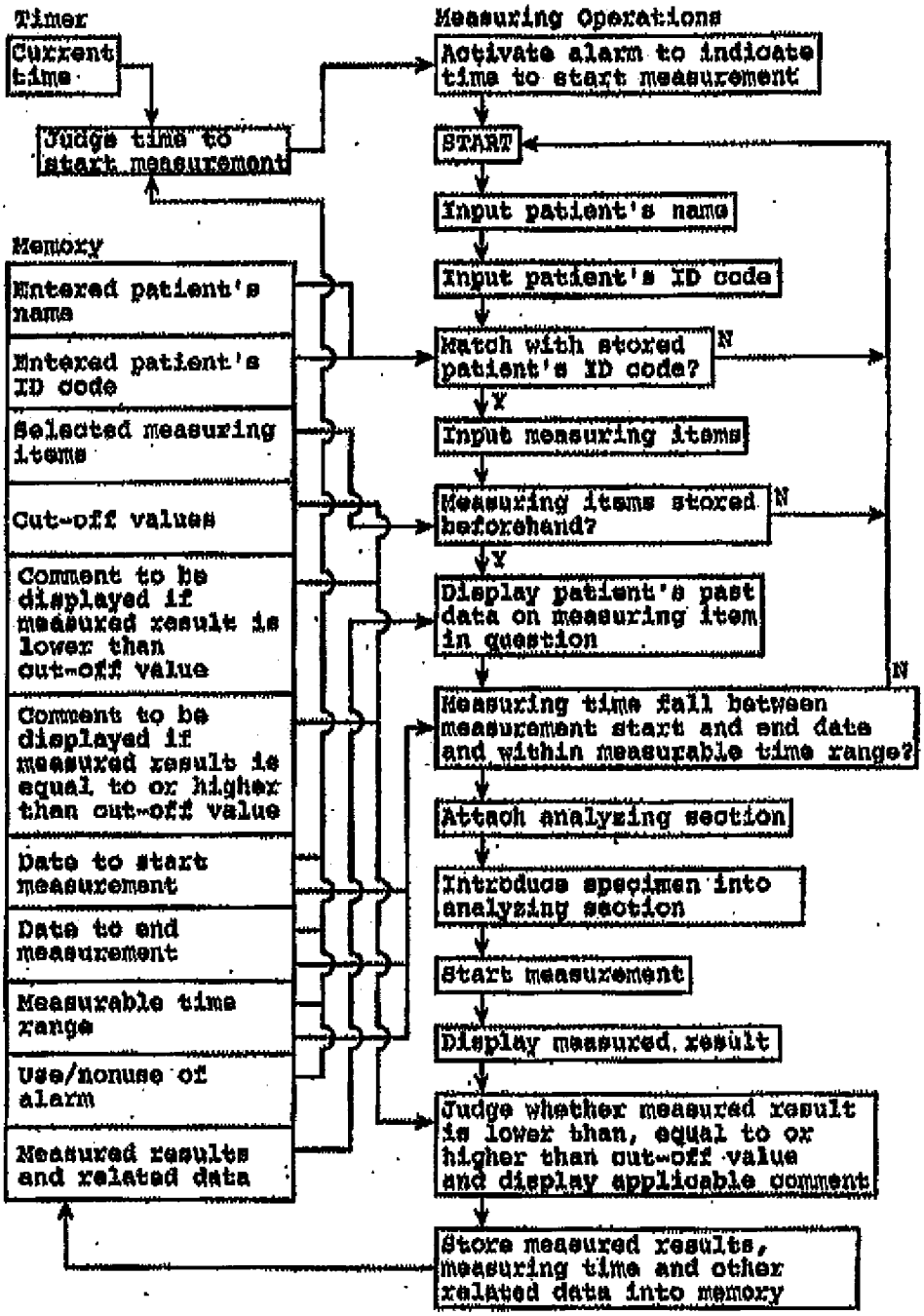

Timer
Current time
Judge time to start measurement
Memory
Entered patient's name
Entered patient's ID code
Selected measuring items
Cut-off values
Comment to be displayed if measured result is lower than cut-off value
Comment to be displayed if measured result is equal to or higher than cut-off value
Date to start measurement
Date to end measurement
Measurable time range
Use/nonuse of alarm
Measured results and related data
Measuring Operations
Activate alarm to indicate time to start measurement
START
Input patient's name
Input patient's ID code
Match with stored patient's ID code?
N
Y
Input measuring items
Measuring items stored beforehand?
N
Y
Display patient's past data on measuring item in question
N
Measuring time fall between measurement start and end date and within measurable time range?
Attach analyzing section
Introduce specimen into analyzing section
Start measurement
Display measured result
Judge whether measured result is lower than, equal to or higher than cut-off value and display applicable comment
Store measured results, measuring time and other related data into memory

FIG. 8

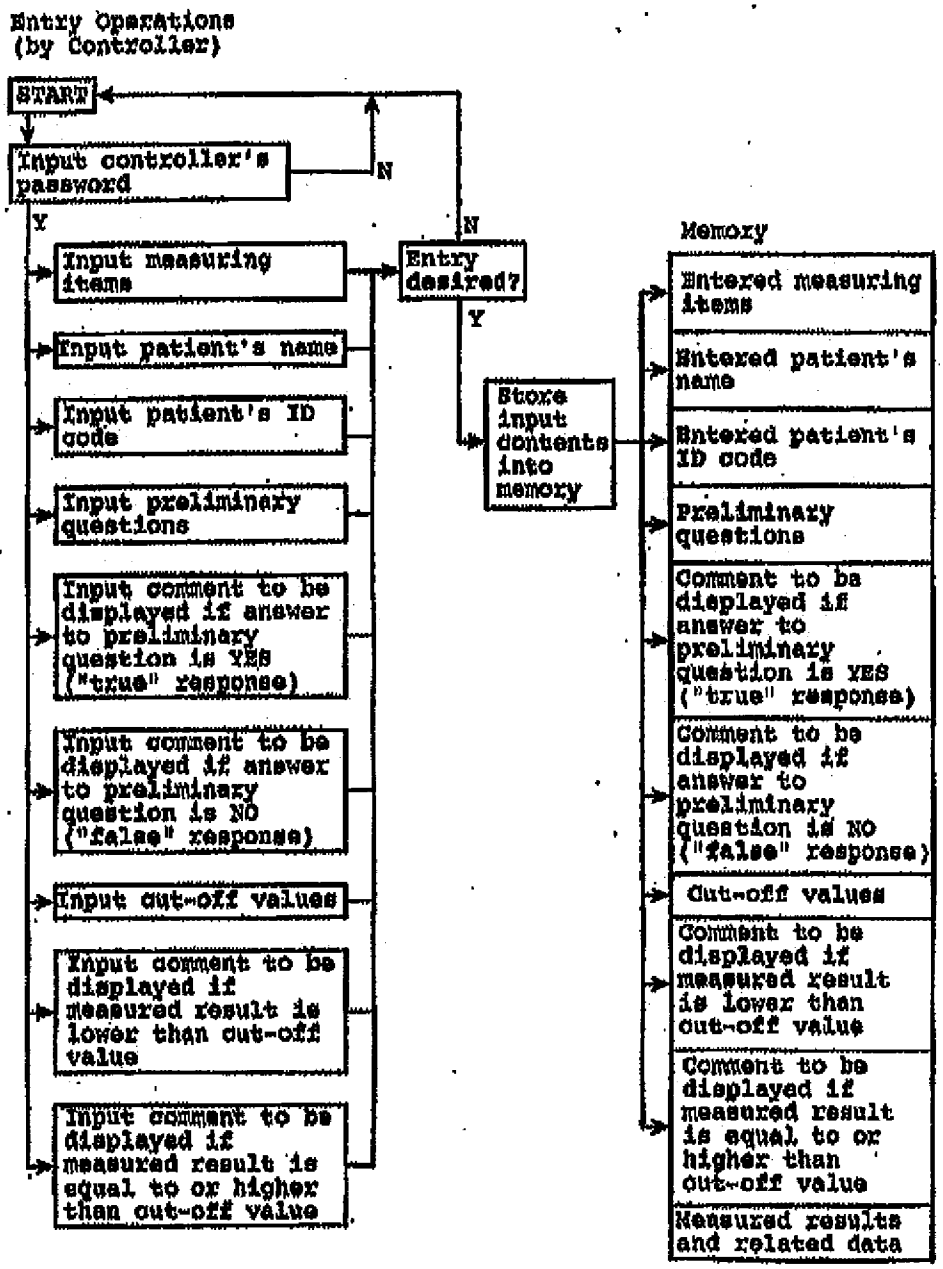

Entry Operations (by Controller)
START
Input controller's password
N
Y
Input measuring items
Input patient's name
Input patient's ID code
Input preliminary questions
Input comment to be displayed if answer to preliminary question is YES ("true" response)
Input comment to be displayed if answer to preliminary question is NO ("false" response)
Input cut-off values
Input comment to be displayed if measured result is lower than cut-off value
Input comment to be displayed if measured result is equal to or higher than cut-off value
N
Entry desired?
Y
Store input contents into memory
Memory
Entered measuring items
Entered patient's name
Entered patient's ID code
Preliminary questions
Comment to be displayed if answer to preliminary question is YES ("true" response)
Comment to be displayed if answer to preliminary question is NO ("false" response)
Cut-off values
Comment to be displayed if measured result is lower than cut-off value
Comment to be displayed if measured result is equal to or higher than cut-off value
Measured results and related data

FIG. 9

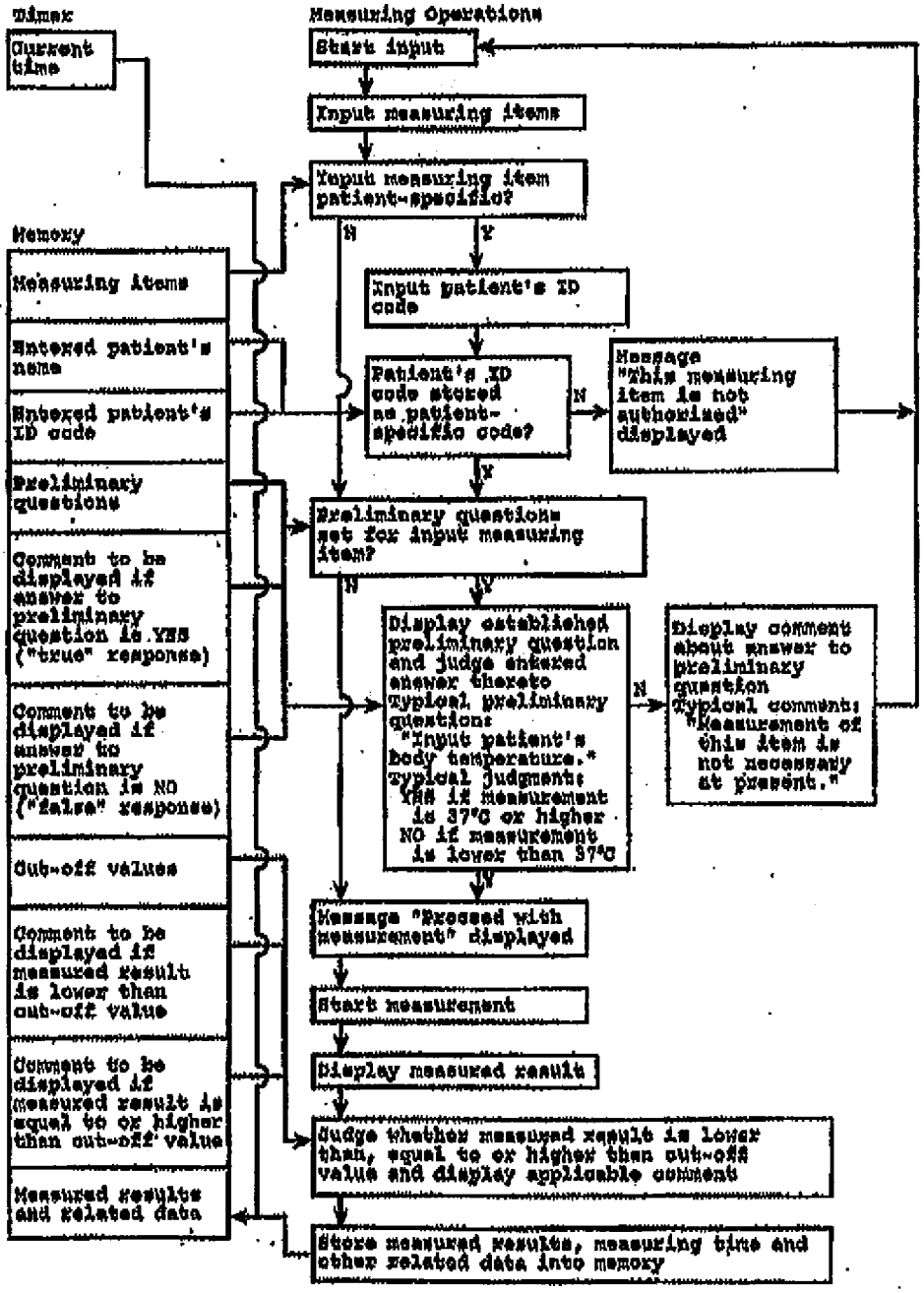

Timer
Current time
Memory
Measuring items
Entered patient's name
Entered patient's ID code
Preliminary questions
Comment to be displayed if answer to preliminary question is YES ("true" response)
Comment to be displayed if answer to preliminary question is NO ("false" response)
Cut-off values
Comment to be displayed if measured result is lower than cut-off value
Comment to be displayed if measured result is equal to or higher than cut-off value
Measured results and related data
Measuring Operations
Start input
Input measuring items
Input measuring item patient-specific?
N
Y
Input patient's ID code
Patient's ID code stored as patient-specific code?
N
Message "This measuring item is not authorized" displayed
Y
Preliminary questions set for input measuring item?
N
Y
Display established preliminary question and judge entered answer thereto
Typical preliminary question:
"Input patient's body temperature."
Typical judgment:
YES if measurement is 37°C or higher
NO if measurement is lower than 37°C
N
Display comment about answer to preliminary question
Typical comment:
"Measurement of this item is not necessary at present."
Y
Message "Proceed with measurement" displayed
Start measurement
Display measured result
Judge whether measured result is lower than, equal to or higher than cut-off value and display applicable comment
Store measured results, measuring time and other related data into memory

FIG.10

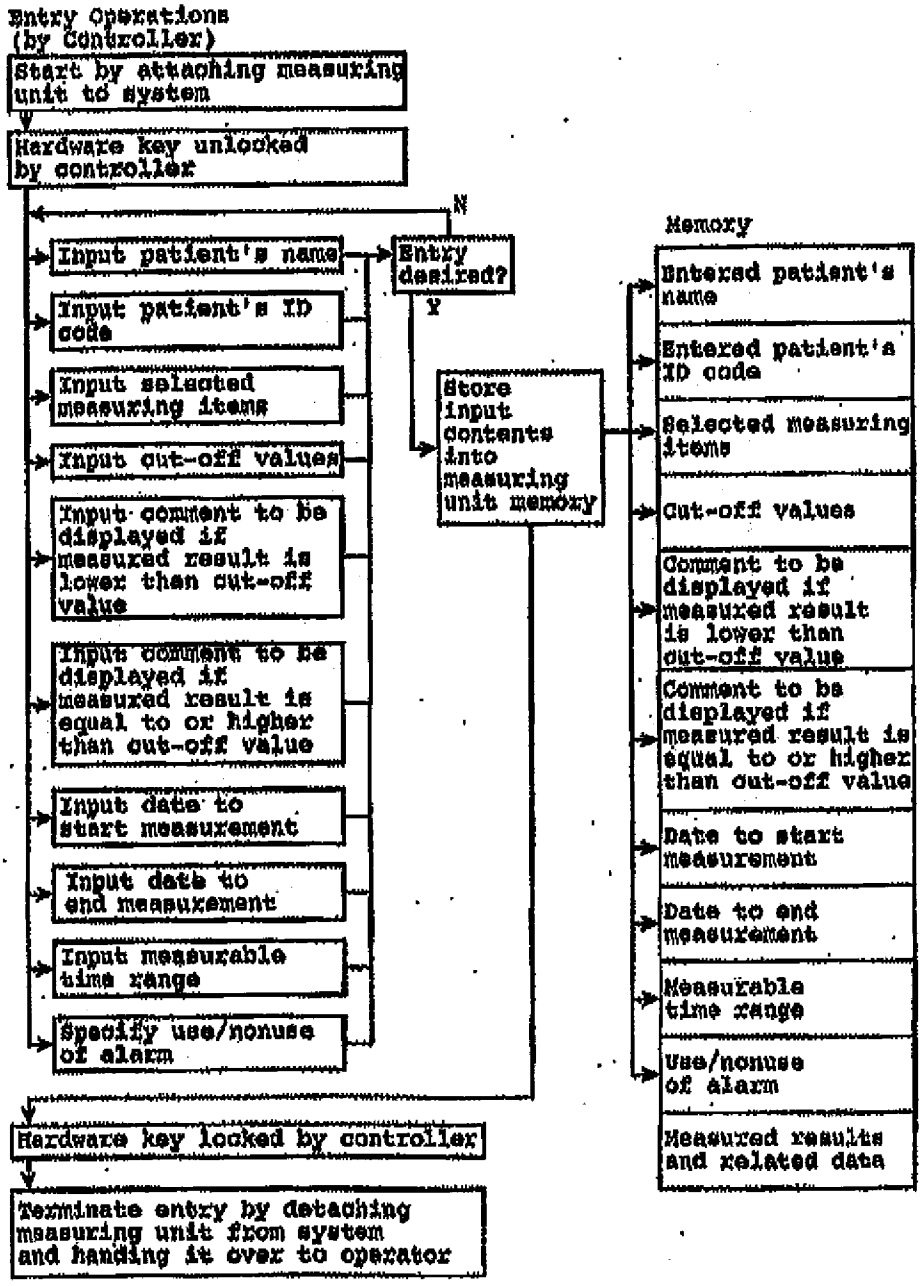

Entry Operations (by Controller)
Start by attaching measuring unit to system
Hardware key unlocked by controller
N
Input patient's name
Input patient's ID code
Input selected measuring items
Input cut-off values
Input comment to be displayed if measured result is lower than cut-off value
Input comment to be displayed if measured result is equal to or higher than cut-off value
Input date to start measurement
Input date to end measurement
Input measurable time range
Specify use/nonuse of alarm
Entry desired?
Y
Store input contents into measuring unit memory
Memory
Entered patient's name
Entered patient's ID code
Selected measuring items
Cut-off values
Comment to be displayed if measured result is lower than cut-off value
Comment to be displayed if measured result is equal to or higher than cut-off value
Date to start measurement
Date to end measurement
Measurable time range
Use/nonuse of alarm
Measured results and related data
Hardware key locked by controller
Terminate entry by detaching measuring unit from system and handing it over to operator

FIG. 11

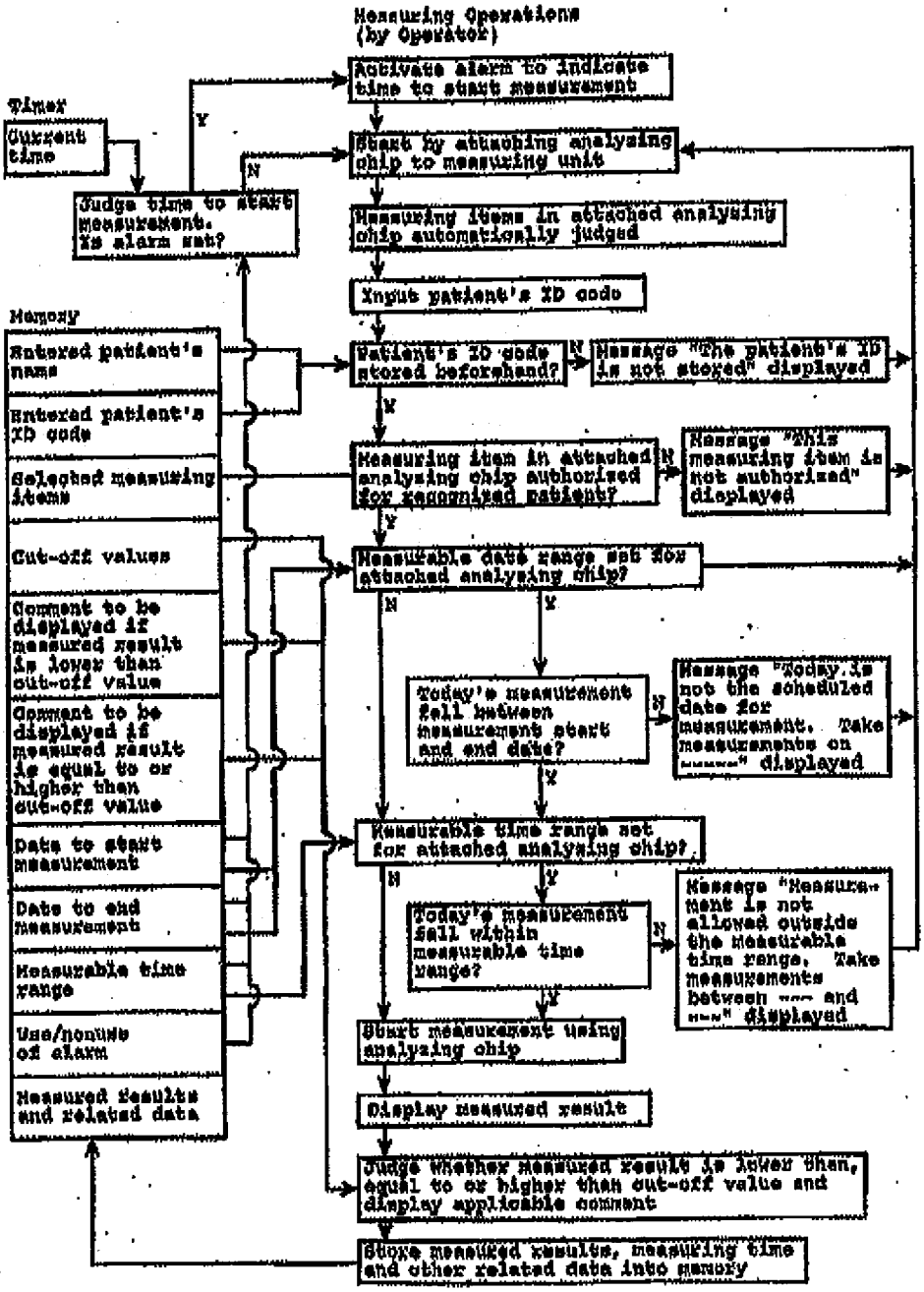

Measuring Operations (by Operator)
Activate alarm to indicate time to start measurement
Timer
Current time
Y
N
Start by attaching analyzing chip to measuring unit
Judge time to start measurement. Is alarm set?
Measuring items in attached analyzing chip automatically judged
Input patient's ID code
Memory
Entered patient's name
Entered patient's ID code
Selected measuring items
Cut-off values
Comment to be displayed if measured result is lower than cut-off value
Comment to be displayed if measured result is equal to or higher than cut-off value
Date to start measurement
Date to end measurement
Measurable time range
Use/nonuse of alarm
Measured Results and related data
Patient's ID code stored beforehand?
N
Message "The patient's ID is not stored" displayed
Y
Measuring item in attached analyzing chip authorized for recognized patient?
N
Message "This measuring item is not authorized" displayed
Y
Measurable date range set for attached analyzing chip?
N
Y
Today's measurement fall between measurement start and end date?
N
Message "Today is not the scheduled date for measurement. Take measurements on ~~~" displayed
Y
Measurable time range set for attached analyzing chip?
N
Y
Today's measurement fall within measurable time range?
N
Message "Measurement is not allowed outside the measurable time range. Take measurements between ~~~ and ~~~" displayed
Y
Start measurement using analyzing chip
Display measured result
Judge whether measured result is lower than, equal to or higher than cut-off value and display applicable comment
Store measured results, measuring time and other related data into memory

FIG.12

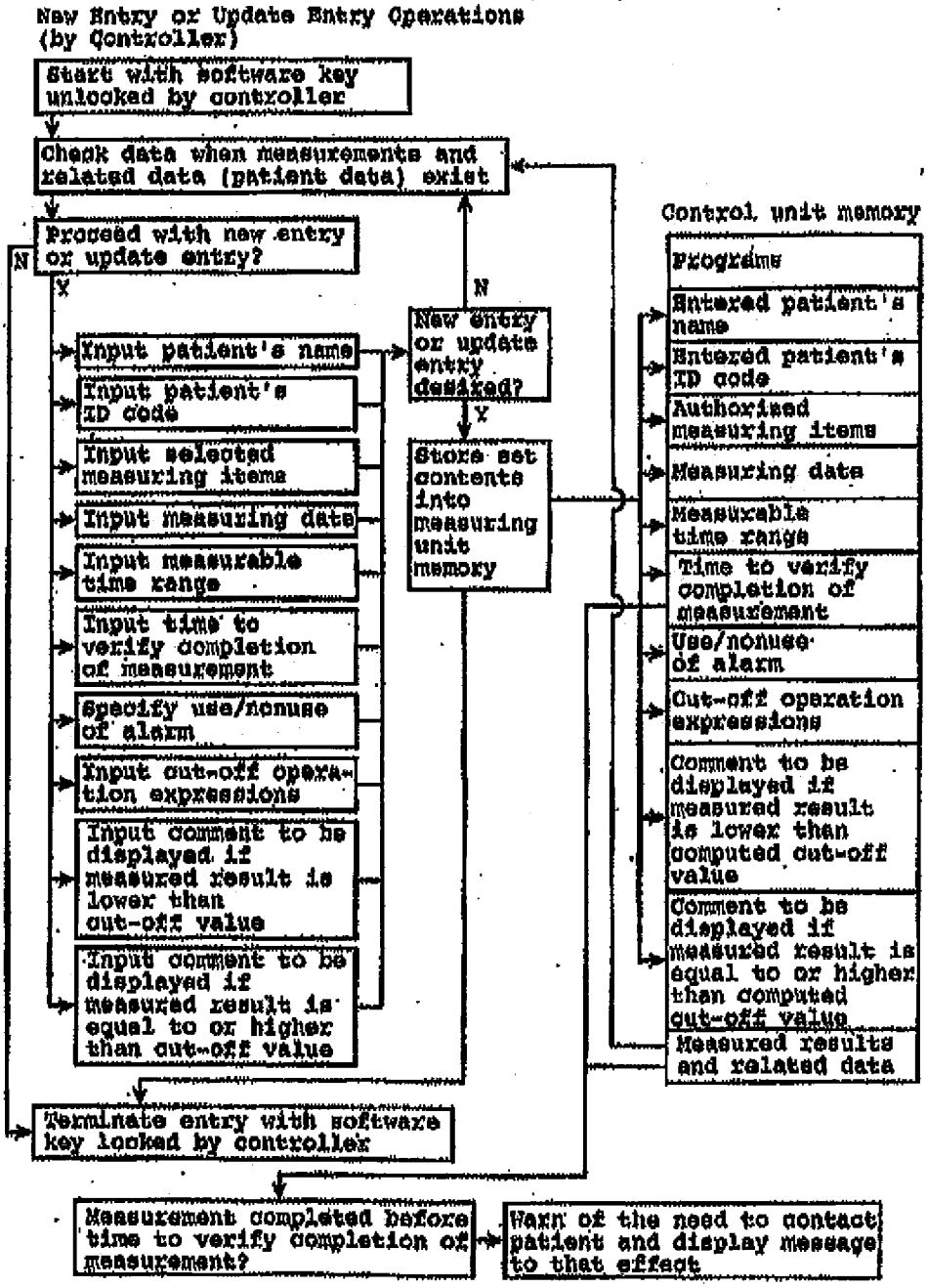

New Entry or Update Entry Operations (by Controller)
Start with software key unlocked by controller
Check data when measurements and related data (patient data) exist
Proceed with new entry or update entry?
N
Y
N
Y
New entry or update entry desired?
Input patient's name
Input patient's ID code
Input selected measuring items
Input measuring date
Input measurable time range
Input time to verify completion of measurement
Specify use/nonuse of alarm
Input cut-off operation expressions
Input comment to be displayed if measured result is lower than cut-off value
Input comment to be displayed if measured result is equal to or higher than cut-off value
Store set contents into measuring unit memory
Control unit memory
Programs
Entered patient's name
Entered patient's ID code
Authorized measuring items
Measuring data
Measurable time range
Time to verify completion of measurement
Use/nonuse of alarm
Cut-off operation expressions
Comment to be displayed if measured result is lower than computed cut-off value
Comment to be displayed if measured result is equal to or higher than computed cut-off value
Measured results and related data
Terminate entry with software key locked by controller
Measurement completed before time to verify completion of measurement?
Warn of the need to contact patient and display message to that effect

FIG.13

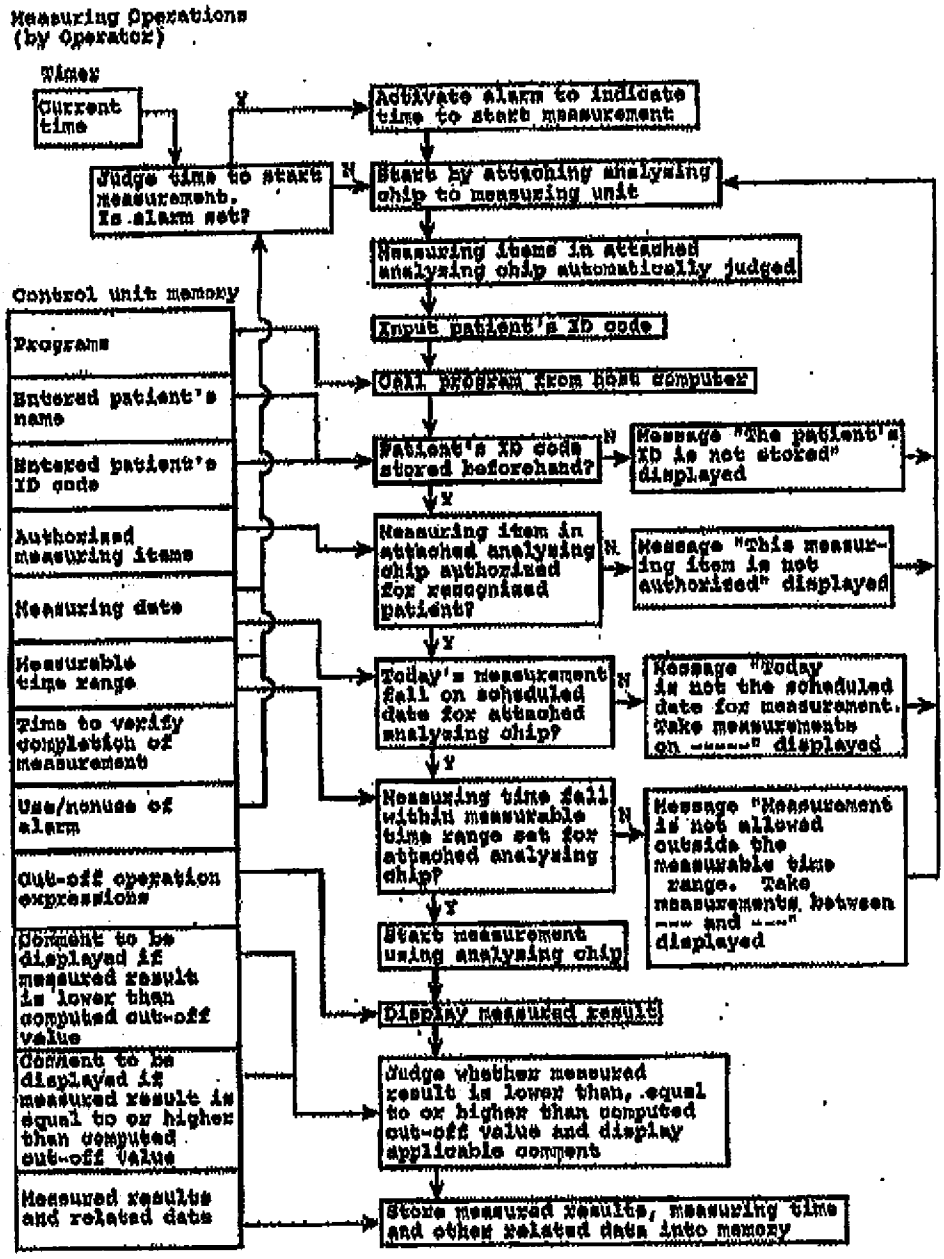

Measuring Operations (by Operator)
Timer
Current time
Y
Activate alarm to indicate time to start measurement
Judge time to start measurement. Is alarm set?
N
Start by attaching analyzing chip to measuring unit
Measuring items in attached analyzing chip automatically judged
Input patient's ID code
Control unit memory
Programs
Entered patient's name
Entered patient's ID code
Authorized measuring items
Measuring date
Measurable time range
Time to verify completion of measurement
Use/nonuse of alarm
Cut-off operation expressions
Comment to be displayed if measured result is lower than computed cut-off value
Comment to be displayed if measured result is equal to or higher than computed cut-off value
Measured results and related data
Call program from host computer
Patient's ID code stored beforehand?
N
Message "The patient's ID is not stored" displayed
Y
Measuring item in attached analyzing chip authorized for recognized patient?
N
Message "This measuring item is not authorized" displayed
Y
Today's measurement fall on scheduled date for attached analyzing chip?
N
Message "Today is not the scheduled date for measurement. Take measurements on ------" displayed
Y
Measuring time fall within measurable time range set for attached analyzing chip?
N
Message "Measurement is not allowed outside the measurable time range. Take measurements between --- and ---" displayed
Y
Start measurement using analyzing chip
Display measured result
Judge whether measured result is lower than, equal to or higher than computed cut-off value and display applicable comment
Store measured results, measuring time and other related data into memory

FIG.14

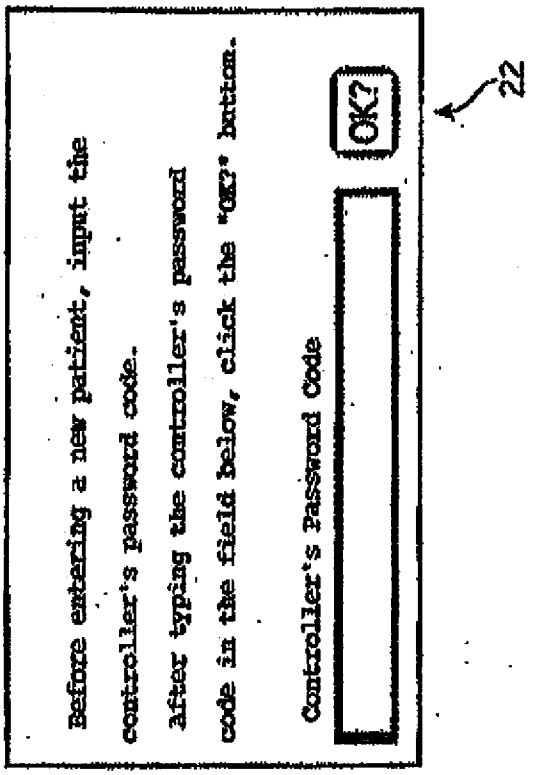

Before entering a new patient, input the
controller's password code.
After typing the controller's password
code in the field below, click the "OK?" button.
Controller's Password Code
OK?
22

FIG.15

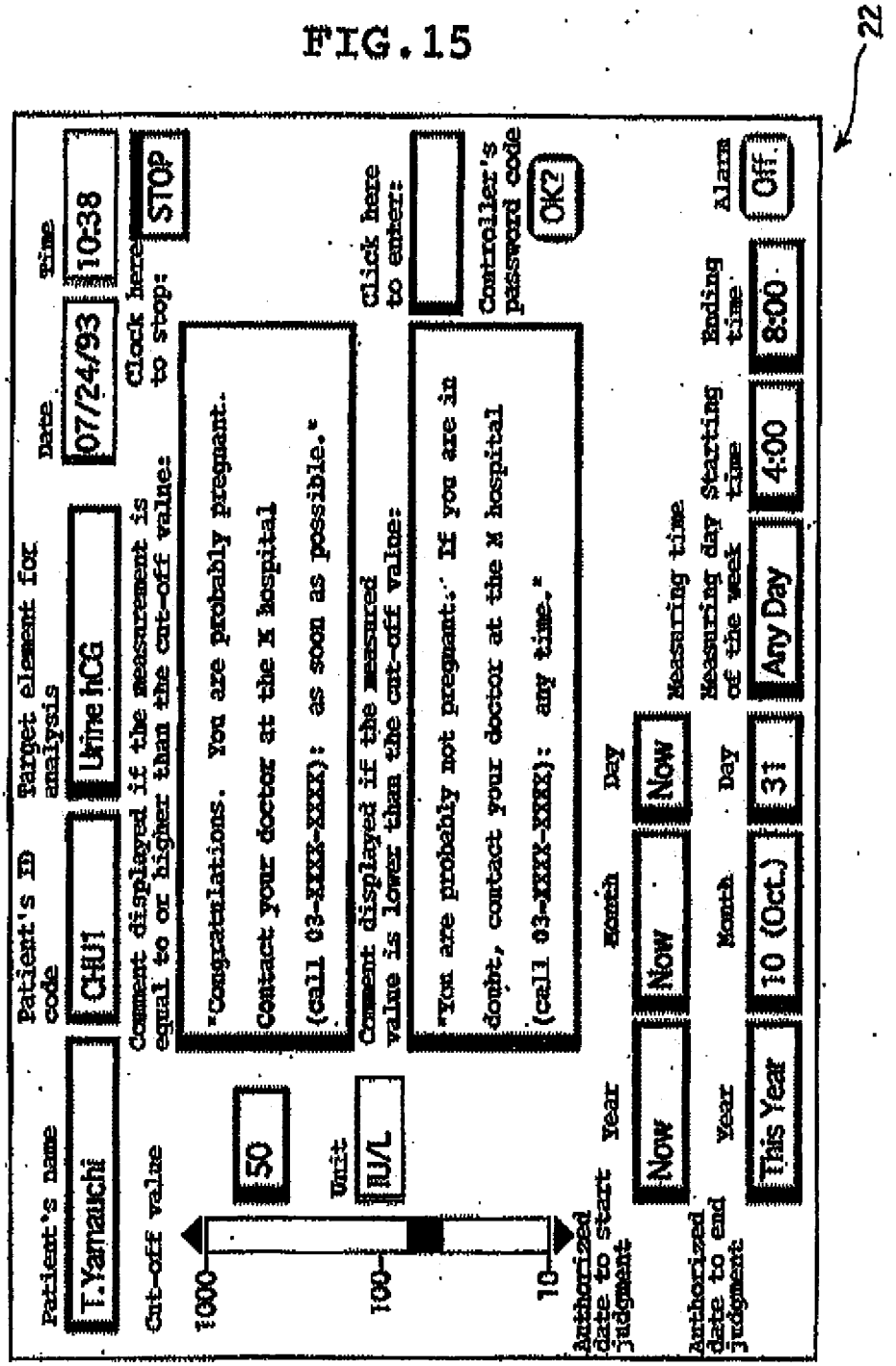

22
Patient's name
T.Yamauchi
Patient's ID code
CHU1
Target element for analysis
Urine hCG
Date
07/24/93
Time
10:38
Cut-off value
1000
100
10
50
Unit
IU/L
Comment displayed if the measurement is equal to or higher than the cut-off value:
"Congratulations. You are probably pregnant.
Contact your doctor at the X hospital
(call 03-XXXX-XXXX); as soon as possible."
Comment displayed if the measured value is lower than the cut-off value:
"You are probably not pregnant. If you are in doubt, contact your doctor at the X hospital
(call 03-XXXX-XXXX); any time."
Click here to stop:
STOP
Click here to enter:
Controller's password code
OK?
Authorized date to start judgment
Year
Now
Month
Now
Day
Now
Measuring time
Authorized date to end judgment
Year
This Year
Month
10 (Oct.)
Day
31
Measuring day of the week
Any Day
Starting time
4:00
Ending time
8:00
Alarm
Off

FIG.16

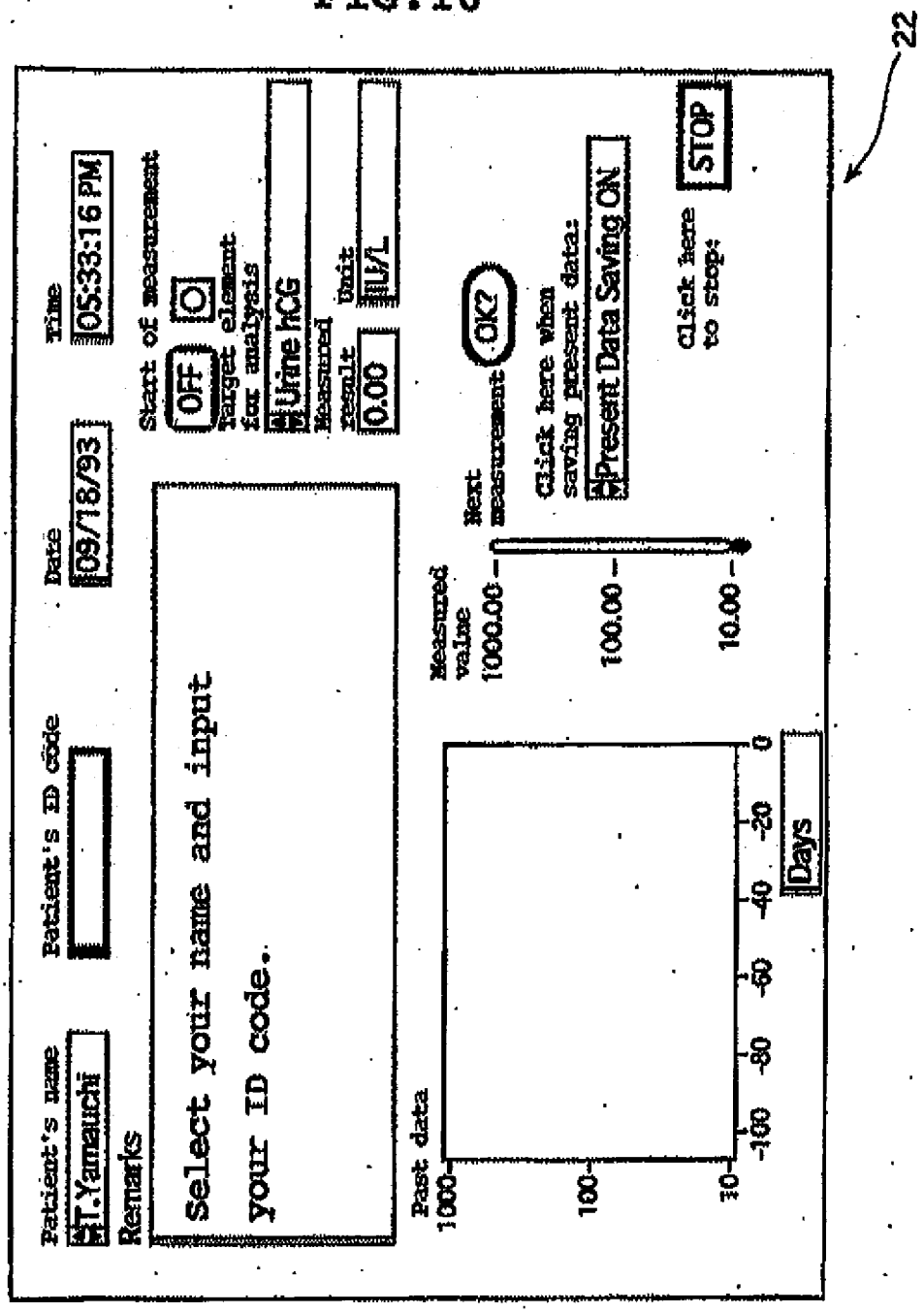

22
Patient's name
T.Yamauchi
Patient's ID code
Date
09/18/93
Time
05:33:16 PM
Remarks
Select your name and input your ID code.
Start of measurement
OFF
Target element for analysis
Urine hCG
Measured result
0.00
Unit
IU/L
Next measurement
OK?
Click here when saving present data:
Present Data Saving ON
Click here to stop:
STOP
Past data
Measured value
1000.00
100.00
10.00
1000
100
10
0
-20
-40
-60
-80
-100
Days

FIG.17

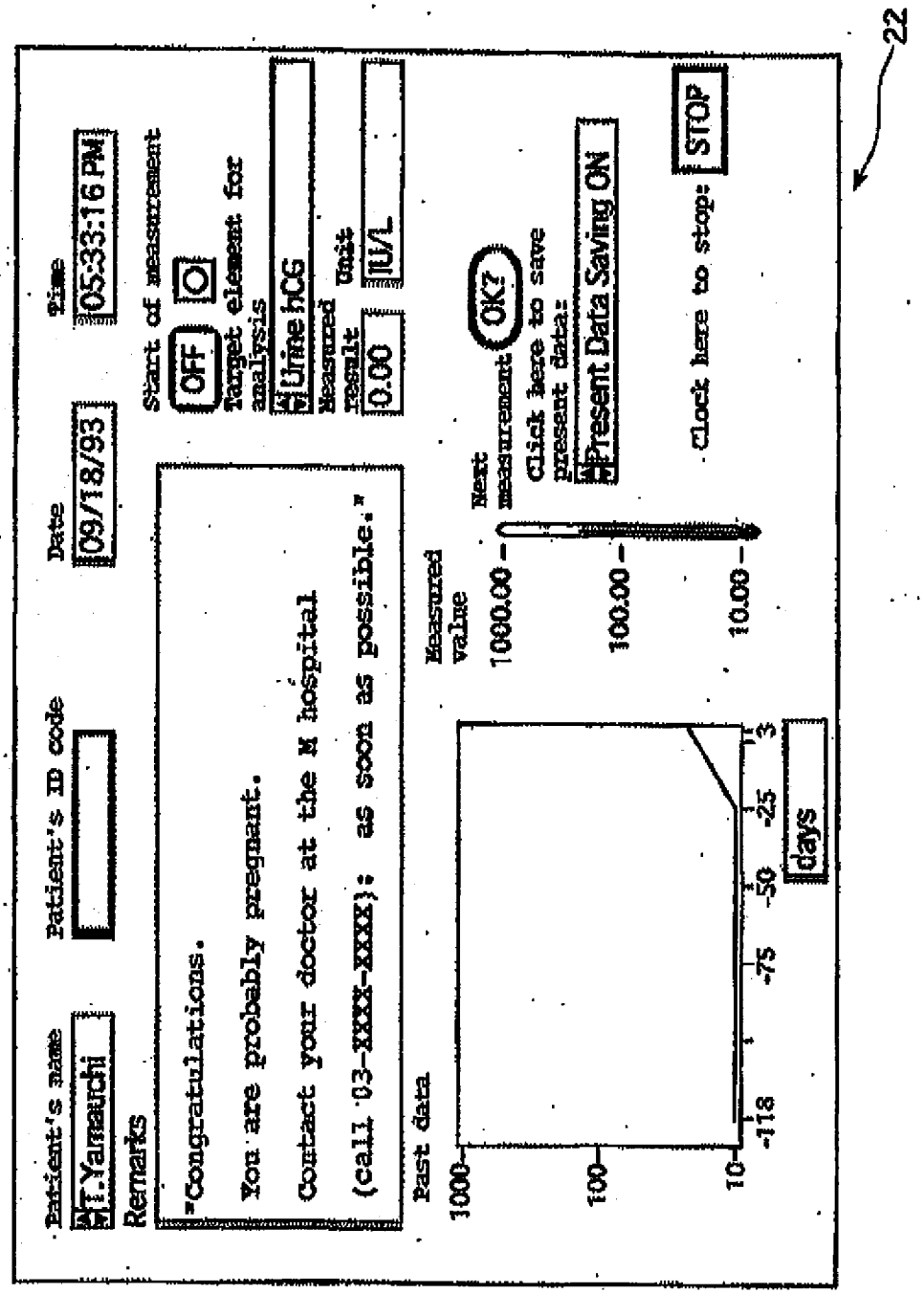

22
Patient's name
T.Yamauchi
Patient's ID code
Date
09/18/93
Time
05:33:16 PM
Remarks
"Congratulations.
You are probably pregnant.
Contact your doctor at the M hospital
(call 03-XXXX-XXXX); as soon as possible."
Start of measurement
OFF
Target element for analysis
Urine hCG
Measured result
0.00
Unit
IU/L
Past data
Measured value
1000.00
100.00
10.00
Next measurement
OK?
Click here to save present data:
Present Data Saving ON
Click here to stop:
STOP
1000
100
10
-118
-75
-50
-25
3
days

FIG.18

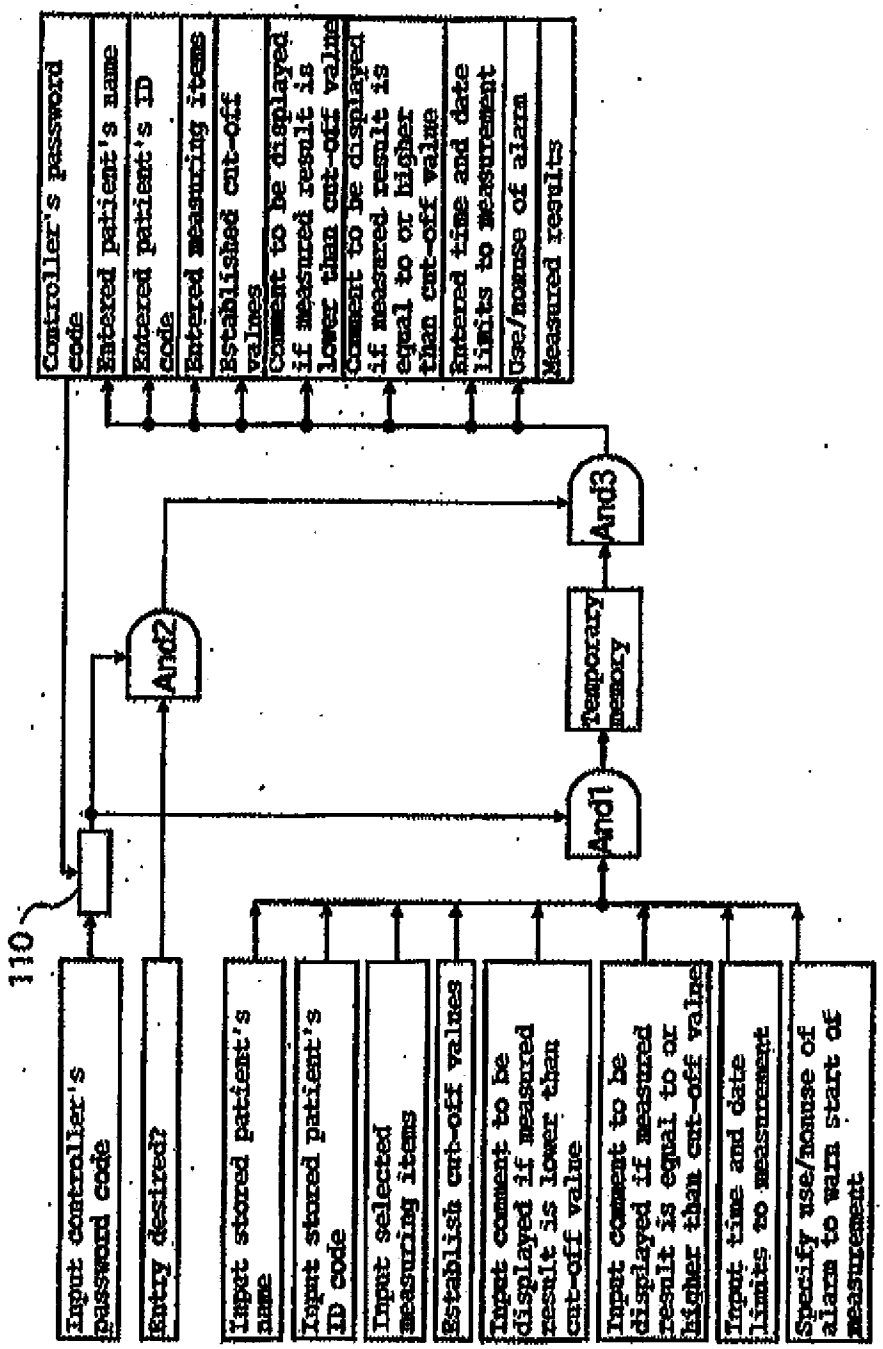
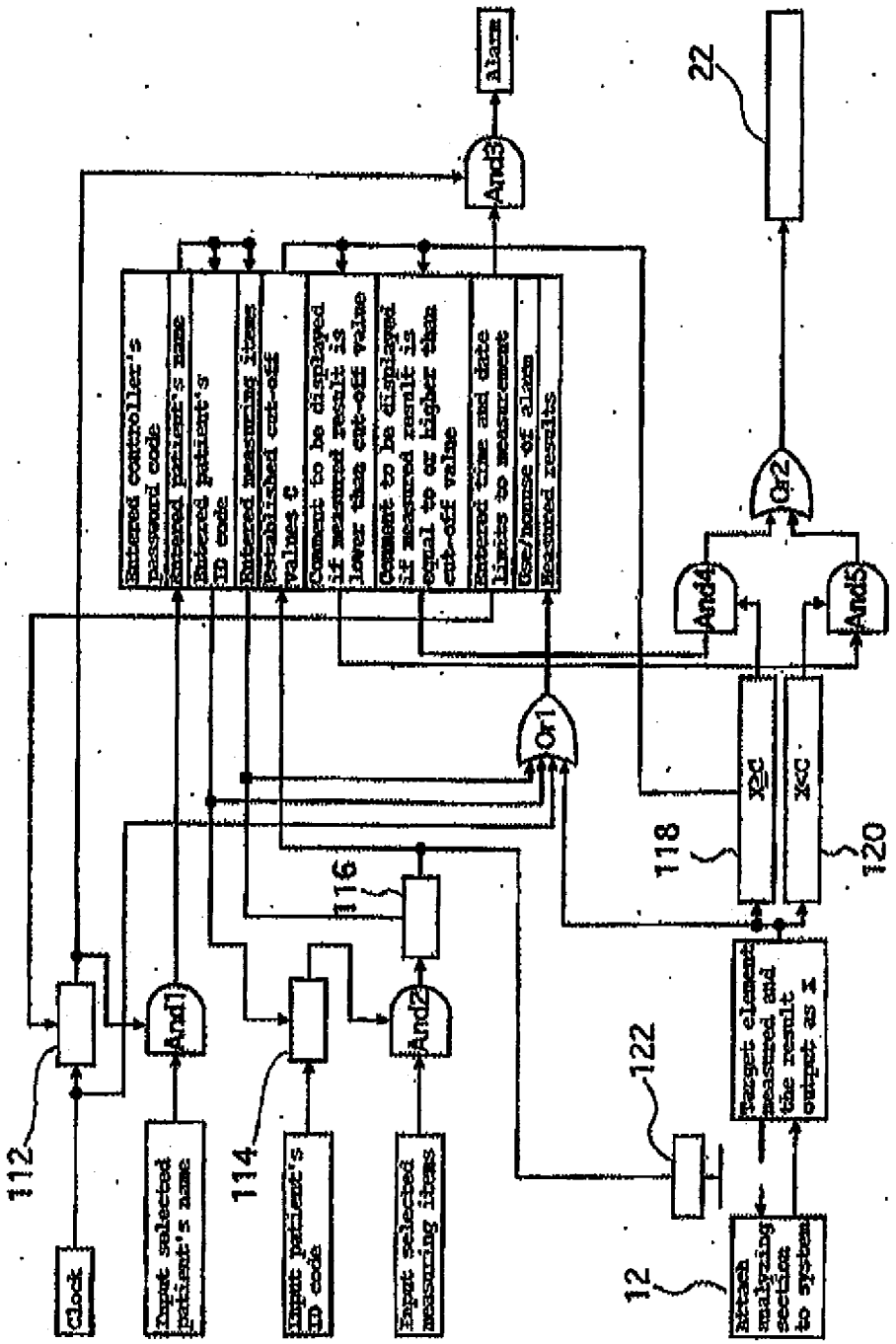

Controller's password code
Entered patient's name
Entered patient's ID code
Entered measuring items
Established cut-off values
Comment to be displayed if measured result is lower than cut-off value
Comment to be displayed if measured result is equal to or higher than cut-off value
Entered time and date limits to measurement
Use/nonuse of alarm
Measured results
And3
And2
Temporary memory
And1
110
Input controller's password code
Entry desired?
Input stored patient's name
Input stored patient's ID code
Input selected measuring items
Establish cut-off values
Input comment to be displayed if measured result is lower than cut-off value
Input comment to be displayed if measured result is equal to or higher than cut-off value
Input time and date limits to measurement
Specify use/nonuse of alarm to warn start of measurement

FIG.19


Clock
Input selected patient's name
Input patient's ID code
Input selected measuring items
And1
And2
And3
And4
And5
Or1
Or2
112
114
116
118
120
122
12
22
Alarm
Entered controller's password code
Entered patient's name
Entered patient's ID code
Entered measuring items
Established cut-off values c
Comment to be displayed if measured result is lower than cut-off value
Comment to be displayed if measured result is equal to or higher than cut-off value
Entered time and date
Limits to measurement
Gender/menses of alarm
Measured results
Xc
Xc
Target element measured and the result output as x
Attach analyzing section to system

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP94/02099

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl[6] G06F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl[6] G06F19/00,A61B5/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926 - 1994
Kokai Jitsuyo Shinan Koho 1971 - 1994

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, A, 4-371134 (Sanyo Electric Co., Ltd.), December 24, 1992 (24. 12. 92) (Family: none)	1-7
X	JP, A, 4-15035 (Toyota Central Research and Development Laboratories, Inc.), January 20, 1992 (20. 01. 92). (Family: none)	1-7
X	JP, A, 4-57161 (Sanyo Electric Co., Ltd.), February 24, 1992 (24. 02. 92) (Family: none)	1-7
X	JP, A, 4-56561 (NTT Data Communications Systems Corp.), February 24, 1992 (24. 02. 92) (Family: none)	1-7
A	JP, A, 4-241028 (Yamatake-Honeywell Co., Ltd.) August 28, 1992 (28. 08. 92) (Family: none)	1-7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"B" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
March 10, 1995 (10. 03. 95)	March 14, 1995 (14. 03. 95)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

C1

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 547 837 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
30.05.2001 Bulletin 2001/22

(51) Int Cl.7: H04L 9/32

(21) Application number: 92311280.0

(22) Date of filing: 10.12.1992

(54) **Document copy authentication**

Authentifizierung einer Dokumentenkopie

Authentification de la copie d'un document

(84) Designated Contracting States:
DE FR GB

(30) Priority: 19.12.1991 US 810644

(43) Date of publication of application:
23.06.1993 Bulletin 1993/25

(73) Proprietor: XEROX CORPORATION
Rochester, New York 14644 (US)

(72) Inventors:
- Merkle, Ralph C.
Sunnyvale, California 94087 (US)
- Bloomberg, Dan S.
Palo Alto, California 94306 (US)
- Brown, John S.
San Francisco, California 94115 (US)

(74) Representative: Grünecker, Kinkeldey,
Stockmair & Schwanhäusser Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(56) References cited:
EP-A- 0 366 867
DE-A- 3 932 097
US-A- 5 157 726

EP 0 547 837 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to a system for making and authenticating a copy of an original document.

[0002] It is known how to authenticate original documents using a digital signature. The latter provides a unique pattern based on the digitized document text and a unique signing key (or secret key) of the document creator. When the original with attached digital signature is transmitted (electronically or as a hard copy) to a third party, the latter through digitizing and processing of the received document and digital signature can determine whether the document is genuine.

[0003] Ways of providing digital signatures of original documents are described in USPs 4,881,264; 4,309,569; 4,625,076; 4,656,474, and other related patents. The digital signature, in effect, is an encoded version of the entire document, reduced to a unique marking added as a seal to the original document. If the original document or its signature is modified in any way, the alterations will be detected when the document and signature are checked with the appropriate decoding key.

[0004] The first of the above-described patents describes a dual-key or public key cryptosystem for generating a digital signature of a document. In this system, the originator or creator uses a private or secret signing key for processing the document by a particular algorithm to generate a "signature" represented by a sequence of bits ranging from several hundred to several thousand depending upon the particular system used and the level of security desired. The receiver of the digital signature would possess or be given a checking or public key, mathematically related to the signing key, which can be used to process the document through a related algorithm to determine whether the received document was indeed generated with the authentic signing key of the creator. If the contents of the document are to be kept secret, then it can be separately encoded and decoded by one of many known encoding and encryption schemes.

[0005] One company has described a so-called time stamp seal (akin to a notary seal) representing a digital signature of the document plus a time stamp to mark the time when the document was received and the digital signature recorded. USP 5,001,752 describes in detail another version of a time notarization system.

[0006] Another company emphasizes the public key cryptography system as a way of achieving a tamper-proof digital signature that can be used to establish the authenticity of electronic mail messages.

[0007] USP 4,650,975 describes a scheme for authentication of an identifying IC card employing a personal identification number (PIN) for checking the validity of a card holder using a Data Encryption Standard (DES).

[0008] The emphasis in the art has been the authentication of original documents or electronic mail messages. There is a much greater need, however, for a reliable scheme to authenticate a hard copy of an original document. The various schemes described above applicable to original documents would not apply to a copy of the document, or at least would not leave a receiver of such a copy with a high level of confidence that the copy in his possession is, in fact, an exact duplicate of some original document located at a distant place.

[0009] A major object of the invention is a system for making or authenticating a hard copy of an original document. Authenticating a copy means verifying that the copy currently in the possession of the receiver is in fact identical to an original document from which the copy was prepared.

[0010] This is achieved, in accordance with one aspect of the invention, by making a copy of the original document on a copying machine that also generates from the original a digital signature that is affixed to the copy, constituting a digitally signed copy of the original document. The digital information can be in human-readable or encrypted form.

[0011] In accordance with another aspect of the present invention, in order to guarantee that the supplier of the original document authorized the making of the signed copy, identifying information unique to the supplier may be required before the copying machine makes the signed copy.

[0012] In a preferred embodiment, a special key known only to the signer or document originator is used to generate the signed copy. A second special key needed to check the signed copy can be included in the signed copy.

[0013] In accordance with a further aspect of the invention, a time stamp can also be included in the digital signature.

[0014] The thus-produced signed copy can then be forwarded by any means and by any person to a receiver at a location, usually distant, where the receiver need have no access to the original document.

[0015] The receiver then processes the signed copy through a similar copying machine that has the capability of storing the unique identifying information of the sender, or of deriving from the signed copy, if incorporated therein, the unique identifying information or related information, such as a checking key as previously described. The resultant processing provides an indication of whether the received copy is an authentic copy of the original. The indication could be as simple as a Boolean output on the machine indicating the processed document is valid or invalid. Alternatively, a message can be displayed on the machine or affixed to a digitally cleaned copy of the signed document that would indicate that the cleaned copy looks like an original document that was copied by a named individual at a certain time and date.

[0016] In accordance with one aspect of the invention there is provided a system for authenticating hard cop-

lies of original documents comprising (a) a copying machine, said copying machine including,

(i) means for receiving from an entity an original document,
(ii) means for generating a digital signature from a document,
(iii) means for receiving information uniquely identifying the entity supplying the original document,
(iv) means for incorporating in the digital signature information representative of the entity's identification,
(v) means for producing a signed document first copy incorporating the digital signature.

[0017] In one embodiment the first copy produced by means of (a) (v) is an encrypted copy of the original document.

[0018] The digital signature may in differing embodiments be either visible or invisible.

[0019] The present invention will be described further, by way of example, with reference to the accompanying drawings, in which:-

Fig. 1A and 1B are schematic views of examples of document authentication schemes, some features of which may be used in the system of the invention;
Fig. 2 is a schematic view illustrating operation of the system in accordance with one embodiment of the invention; and
Fig. 3 is a block diagram of a copying machine usable in a system in accordance with one embodiment of the invention.

[0020] Information integrity has been a persistent challenge now for several decades. For example, in transmitting digital information, a checksum based on a computation of the digital information in accordance with some arbitrary algorithm could be added at the end of the transmission. The receiver of the digital data would perform the same computation and then compare its computed checksum to that included in the transmitted data. Any discrepancy indicates that the received data is not an exact replica of the transmitted data.

[0021] Any document can be digitized in any of several known ways. For instance, if the document is wholly of text, it can be converted to a stream of ASCII codes and subsequently digitized. If, instead, non-standard textual symbols are used, or non-textual, or graphical information is present in the document, the document can be digitized by known scanning processes based on black/white or dark/light transitions. That stream of digital information representing the document contents can be subjected to a checksum, hashing or similar algorithm or function whose output would then represent the actual full contents of the document. Similarly, digital information can be encoded and digitally signed. Both the digital information and the digital signature can then be encoded and printed onto a sheet of paper. The information encoded and printed onto the paper can include; for example: description of what is printed on the document (allowing verification of document content); descriptions of the physical nature of the document (allowing controlled copying and distribution of the document); or descriptions of programs that are to be loaded into and executed by the machine reading the document (whether that machine be a FAX, copier, scanner, etc.).

[0022] These efforts have been focussed on establishing the authenticity of original information or data. For example, adding a digital signature to an original document can be used to authenticate the original.

[0023] Encryption is another technique for assuring integrity of transmitted information, often used nowadays for secure electronic transmission of data or for E-mail. Many encryption schemes are known and are used today. One of the more popular schemes uses the dual public/private key system. Figs. 1A and 1B illustrate how such a system could be employed to verify the authenticity of an original document, such as a check or IOU.

[0024] Referring now to Figs. 1A and 1B, in the process illustrated in Fig. 1A, a document 10, which may be, for instance, an IOU for $1,000, is created as an original document. The document 10 is then scanned and digitized together with a secret signing key possessed only by the creator of the document. After being processed by one of many well known signing algorithms indicated at 11, the result is a digital signature which can be incorporated with the document or as part of the original document 10. The original document 10 with the digital signature is indicated at 12, separate from or included as part of the document 10. The latter can then be transmitted to a third party who would possess a public checking key counterpart to the secret signing key as part of this known dual key security scheme. The document would again be scanned and digitized, and the digital signature 12 together with the public checking key processed via a checking algorithm 13. This algorithm, of which again a number are known, would determine whether or not the digital signature received corresponds to that obtained directly from the original document and that the keys used by the creator and by the third party or user properly match in accordance with the checking algorithm. The output of the checking algorithm is a single bit, indicating that the signature is valid or invalid. In an actual embodiment, the output indicating an invalid signature could be a red light, or some other clearly visible indicator that the signature failed the validation check.

[0025] Fig. 1B shows a similar scheme but in this case the document 10 has been altered 10' by changing the amount of money listed on it. When processed as the original unaltered document 10, the checking algorithm would indicate a discrepancy in the document or in the document's source with an appropriate message as indicated at 15 in Fig. 1B.

[0026] To the best of our knowledge, there does not exist a way of providing to a third party a hard copy of an original document and proving that that hard copy is in fact an exact copy of an original document which exists at some other location. This is precisely where the invention of the present case comes into play.

[0027] Fig. 2 illustrates schematically the operation of a preferred form of the system of the invention for authenticating hard copies of documents. In this preferred embodiment, an original document 20 is placed on a special machine 25 referred to herein as a signing copying machine or copier. While hereinafter will be disclosed an example of the system contents of a signing copier that can be used in the invention, it will be understood that the exact manner by which the signing copier makes copies of documents, or generates digital signatures of documents is not critical to the invention as any of the known copying and digitizing schemes can be used for this purpose.

[0028] In this particular case, the signing copier 25 has the ability of not only executing a normal copying function and producing or outputting a hard copy of the original document 20, but in addition it has the ability to digitize the document and generate a digital signature of that document in the manner as previously described. That digital signature of the document includes every significant piece of information on the document, as well as information that is unique to the signer, which may be a person or a group, such as a secret signing key.

[0029] In addition, the signing copier 25 can include the further feature that it has the capability of verifying the identity of the person or entity that supplies the document to the signing copier. In this particular case, we assume that the possessor of the document 20 is a person named "John Doe". John Doe has a smart card with which he can activate the signing copier 25. The smart card can be one of many different kinds of well known articles which can be inserted into a slot in the signing copier, which in turn would read certain data on the card representing the identity of that owner to be incorporated in the digital signature that is prepared from the original document 20. John Doe's secret key can be included in his smart card, as well as the signing algorithm and his public key. Alternatively, the signing algorithm can be included in the signing copier 25.

[0030] That digital signature which now includes the identification of the document supplier John Doe is now affixed 33 to the hard copy produced by the signing copier machine 25. That hard copy, designated 35, is a "signed document", meaning a document which has on it in visible or invisible form a digital signature 33 of the document contents together with an identification of the supplier or creator. Moreover, the original document 20 can be in human readable form, or encrypted for secrecy, in which case the signed document 35 would also be in human-readable or encrypted form.

[0031] The signed document 35 or hard copy can then be forwarded 31 by any known means to a third party, such as by hand delivery, or by use of one of the postal or other delivery services. That signed document 35 when received by the third party is again processed through a similar signing copier machine 25. What the signing copier machine 25 would do with the signed document 35 is essentially to digitize the contents, and check the digital signature 33.

[0032] A digital signature, by its very nature, requires the signer to have for validation a public checking key that is mathematically related to his private key. The signing copier would obtain, by any one of several means known and described in the literature, a valid copy of the signer's public checking key. As an example, but in no way the only possible method, the signer's public checking key and a "certificate" for the signer's public checking key could both be included in the original document in computer readable form. The signing copier 25 would read both the certificate and the public checking key and would validate the certificate and public checking key using a well known Public Checking Key (which can be owned by the copier manufacturer). Having validated the public checking key of the signer, the digital signature of the signer and the validity of the digital information signed by the signer could then be checked.

[0033] Alternatively, the public checking key of the particular signer could be made publicly available, as in a directory or the like, and accessed by the signing copier 25.

[0034] The output from the second signing copier used by the third party would typically be a digitally cleaned document 40, meaning a hard copy of the original document 20 free of any physical dirt or image fuzziness introduced during handling and processing of the original or signed document. This is readily accomplished because the information needed to clean the copy and restore the original was digitally encoded on the copy and thus the signing copier can readily determine what the original document actually looked like. In addition, there can be imprinted on the digitally cleaned document 40 by the signing copier a message indicating that the digitally cleaned document 40 looks like an original document that at a certain time and on a certain date was copied on a signing copier machine with the authorization of John Doe. Alternatively, the message can be omitted from the document and instead displayed on the machine. The machine could be readily programmed not to make hard copies of signed documents unless they have been properly verified in accordance with the invention. In this latter case, third parties or users would know that any copy produced by such a machine from a signed document is identical to an original signed document at some other location.

[0035] As mentioned previously, there are many known ways by which the various functions described above can be implemented, and the invention is not limited to the specific means by which the digitization, optical copying, comparison systems, and other verifying

features are implemented. Fig. 3 shows schematically one relatively simple machine 25 which would have a space, say, on top for receiving a document which may be an original document 20 or a signed document 35, a keyboard 60 for keying in appropriate commands or instructions to the machine where necessary, and a conventional card input device 61 through which an identifier object, such as a smart card, can be passed from which information concerning the secret signing key and other information can be verified by conventional means indicated in Fig. 3 by block 62. The signing copier 25 would have the usual optical copying means 64 which would be capable of making a copy of a document. That copy could be a literal copy of the document. The exact form is not important to the invention. The processing is controlled by a conventional programmable processor 65 which, for simplicity, is not shown connected to, for example, the keyboard 60 or the card input device 61, or the ID verifier 62, or the other modules employed in the machine. The means to accomplish this would be obvious to one of average skill in the art. The signing copier would also possess a conventional scanner so that it would be capable of digitizing the information present on the document indicated at block 66. It could at the same time, optionally, encrypt at block 67 the document contents. It could also have present at 60 a device which keeps track of the current date and time of day which information can be retrieved and used whenever desired.

[0036] The signing machine 25 illustrated in Fig. 3 is capable of carrying out both sets of functions indicated in Fig. 2 in which it can produce not only the signed document 35 but also the digitally cleaned document 40 which has been authenticated. Thus some of the modules indicated in Fig. 3 would only be used at the sending end when the original document is hard copied, whereas other modules would be used at the receiving end where the digitally cleaned and authenticated hard copy of the signed document is produced. Alternatively, two different machines could be provided, one just for creating signed documents at the sending end, and the other at the receiving end for verifying the authenticity of a signed document and producing a digitally cleaned document.

[0037] Continuing with the description, at block 62 the resultant digital signature can be generated by processing with any known algorithm with the secret signing key of the user to generate a digital signature which can be affixed to the optical copy that has been made of the original document. This merger of the optical copy with the digital signature occurs at block 64. In addition, further information could be included in the digital signature, e.g., a time stamp which would indicate the date and the time when the signed document was produced.

[0038] At the receiving end, the document 35 placed on the machine would be the signed document, and in this case the function of the machine would be to make sure that the digital signature that appeared on the signed document is valid. To do this, as previously described, the copying machine must obtain a valid copy of the signer's public checking key.

[0039] After the digital signatures have been checked at block 66 will determine the next stage in the processing. There are a number of possibilities here. For example, if the digital signature is not valid, then the machine is readily programmed not to copy it, and to display on the machine a message saying that the hard copy originally presented to the machine has not been authenticated.

[0040] On the other hand, where the digital signature checks, and the original supplier was authorized, then the machine could display a message 68 indicating that a hard copy produced by the machine is identical to one that was presented to a similar machine at a certain time and date. For instance, the message could read "This document (meaning the outputted digitally cleaned copy 40) was submitted for copying by John Doe on May 9, 1991 at 1:55:35 p.m. When it was submitted, it looked like the herewith supplied copy." Alternatively, the message can be put on the document itself. As a further alternative, both forms of informing the third party user of the authenticity of the hard copy of the document can be employed.

[0041] Thus, in the system of the invention, any user document can be supplied to the machine for authentication. The signed document contents can have digital information encoded in it either in visible or invisible form. Many users of such machines would be available whose authority is readily established by being issued a card which is authenticated by the machine supplier. While a smart card is a preferred way of inputting the signer's secret signing key, in principle, the keyboard 60 can also be employed to carry out the same function by means of known password schemes. It would be possible though not essential for the signing copier machine manufacturer to issue and authenticate the smart cards of the users. At the receiving end, the signed documents would be entered for verification and the signing copier would recover the digital information encoded in the document and verify the supplier or creator.

[0042] Summarizing the preferred embodiment, a digital signature system may be thought of as two functions:

(i) signature = SIGN(document, signingKeyOfA), and
(ii) valid = CHECK(document, signature, checkingKeyOfA), where:

"document" means any sequence of bits;
"signingKeyOfA" means secret information known by A which allows A (and nobody else) to generate valid signatures;
"signature" is a sequence of bits generated by the signing algorithm, with the number of bits ranging from a few hundred to a few thousand, depending on the specific system and the spe-

ofits security level involved in the application, as well as various performance tradeoffs; "checkingKeyOfA" is mathematically related to the signingKeyOfA, where user A would generate both the signing key and the checking key, and the signing key would be kept secret, while the checking key would be made public;

[0043] The "valid" flag is a simple boolean, either TRUE or FALSE. If the signature for a given document was generated by signingKeyOfA, then the CHECK function will return TRUE, indicating that everything is OK. If the signature or document has been altered in any way, then the CHECK function will return FALSE, indicating that the signature is not valid.

[0044] The following scenario is illustrative of how such applications could work and represents an algorithm describing a preferred form of the overall performance of the system:

1) The customer prepares a document, such as a signed contract, and approaches the Signing Copier.

2) The customer inserts their "signing card" into the copier, and places the original on the glass. The copier digitizes and compresses the image, signs the compressed image, and stores the signed compressed digital image in a user inconspicuous fashion on the resulting "copy" (actually a "signed original").

3) Further hard copies can now be made of the signed original, and as long as the image quality is not too degraded by repeated copying; the original digital information can be recovered from the copy and verified.

4) The special signing copier machines would recover the digital information, restore the quality of the document, and verify the authenticity of the document. Other conventional copiers could simply copy the document.

5) The "signed" nature of the document could be indicated by using special ink or special hard-to-duplicate patterns. In this fashion, the fact that the document was signed would be readily apparent on visual inspection. The physical nature of this user-obvious indicator does not affect the logical design of the system.

6) This scenario assumes that a reasonable key authentication protocol is used by the copier. In particular, it assumes that the "signing cards" issued to customers can be appropriately authenticated by a suitable entity, such as the signing copier manufacturer or supplier. The simplest method of doing this would be to issue such "signing cards" directly from the machine supplier, charging some modest price. The customer would have to present documentation adequate to persuade the supplier that they were indeed who they claimed to be, after which they would be issued a signing card. The signing cards issued by the supplier could be readily identified by any supplier's copier as authentic, but it would be impossible for any non-supplier agency (legitimate or otherwise) to issue a signing card that any supplier's copier would think was authentic.

7) The recipient of a signed copy could easily verify that it was authentic by placing it in any Signing Copier, which would verify the accuracy of the document.

8) Optionally, if desired, the signed information could describe some physical aspect of the piece of paper on which it appeared. In this way, it would be impossible to make authenticated duplicates. Known ways of doing this have been based on the pattern of fibers in the paper as a physically unique identifier for that particular piece of paper. In this scenario the agent that deals with the customer might be thought of as a "notary public" who happens to be employed by the supplier. The signing card issued to the customer can be "tamper proof, " so that the customer is unable to access its contents. The signing card may have an on-board microprocessor and memory which implement the necessary algorithms. The possession by the customer of the signing card is evidence that the customer is who they claim to be Further authentication might be required, e.g., the customer might also have to know a password, or the customer's fingerprint might be encoded in the signing card and verified by the copier. The signing copier authenticates the signing card, and might perform further authentication as needed (e.g., ask for a password or check the fingerprints). The copier would then be prepared to issued documents that had been digitally signed by the customer. From a technical point of view, changing any bit at all in either the document or the signature will invalidate the signature. If a single pixel is out of place in the image, the signature will be invalid. In practice, this means some form of error correcting code will almost certainly be required if the digital information is stored on paper. Paper can have dirt, grease, coffee, etc. spilled on it, and unless the error correcting code is quit robust, this would invalidate the signature.

[0045] For more information on digital signatures and means for implementing same, reference is made also to Matyas "Digital Signatures - An Overview", Computer Networks 3(1979) pp. 87-94, particularly Sect. 3; and Lipton et al "Making The Digital Signature Legal-And Safeguarded", Data Communications, February 1978, pp. 41-52, especially pp. 44, 47.

[0046] While the invention has been described and illustrated in connection with preferred embodiments, many variations and modifications as will be evident to those skilled in this art may be made therein without departing from the invention, and the invention as set forth

in the appended claims is thus not to be limited to the precise details of construction set forth above as such variations and modifications are intended to be included within the scope of the appended claims.

Claims

1. A process for making an authenticatable hard copy duplicate (35) of an original document (20) supplied by an entity, comprising:

copying the contents of said original document (20) on said hard copy (35), and

incorporating on said hard copy (35) a digital signature (36) representing said contents and the identity of said entity.

2. A process for authenticating an authenticatable hard copy duplicate (35) made of an original document (20) supplied by an entity and comprising the contents of said original document (20) and a digital signature (36) representing said contents and the identity of said entity, said process comprising:

checking said digital signature (36) on said hard copy duplicate (35), and

indicating whether said hard copy duplicate (35) is authentic.

3. A process as claimed in claim 2, further comprising:
if said hard copy duplicate (35) is authentic, copying said contents but not said digital signature (36) on at least one other hard copy (40).

4. A process as claimed in claims 1 to 3, wherein:
said digital signature (36) is generated using dual-key authentication with a secret signing key representing said entity.

5. A process as claimed in claim 4, wherein
said authenticatable hard copy duplicate (35) further comprises a public key that is mathematically related to said secret signing key.

6. A unit for making an authenticatable hard copy duplicate (35) of an original document (20) supplied by an entity, comprising:

means for receiving said original document (20) from said entity,

means (54) for copying the contents of said original document (20),

means (60,61) for receiving information uniquely identifying said entity,

means (52) for verifying said information,

means (58,62) for generating a digital signature (36) representing said contents and the identity of said entity, and

means (64) for producing said hard copy duplicate (35) comprising said contents and said digital signature (36).

7. A unit as claimed in claim 6, wherein:
said means (62) for generating said digital signature (36) uses dual-key authentication with a secret signing key representing said entity.

8. A unit as claimed in claim 7, further comprising:
means for incorporating a public key that is mathematically related to said secret signing key on said hard copy duplicate (35).

9. A unit for authenticating an authenticatable hard copy duplicate (35) made of an original document (20) supplied by an entity and comprising the contents of said original document (20) and a digital signature (36) representing said contents and the identity of said entity, said unit comprising:

means for receiving said hard copy duplicate (35), and

means (56,58) for checking said digital signature (36).

10. A unit as claimed in claim 9, further comprising:
means (60) for indicating whether said hard copy duplicate (35) is authentic.

11. A unit as claimed in claim 9 or 10, further comprising:
means for copying said contents but not said digital signature (36) on at least one other hard copy (40), if said authenticatable hard copy duplicate (35) is authentic.

Patentansprüche

1. Verfahren zum Erzeugen eines authentifizierbaren Hartkopieduplikats (35) eines Originaldokuments (20), das durch eine Entität bereitgestellt wird, wobei das Verfahren folgende Schritte umfaßt:

Kopieren des Inhalts des Originaldokuments (20) auf die Hartkopie (35), und

Einfügen einer digitalen Signatur (36) auf der

Hartkopie (35), wobei die digitale Signatur (36) den Dokumenteninhalt sowie die Identität der Entität wiedergibt.

2. Verfahren zum Authentifizieren eines authentifizierbaren Hartkopieduplikats (35), das aus einem Originaldokument (20) erzeugt wird, das durch eine Entität bereitgestellt wird, und den Inhalt des Originaldokuments (20) sowie eine digitale Signatur (36) umfasst, welche den Dokumenteninhalt sowie die Identität der Entität wiedergibt, wobei das Verfahren folgende Schritte umfasst:

Prüfen der digitalen Signatur (36) auf dem Hartkopieduplikat (35), und

Angeben, ob das Hartkopieduplikat (35) authentisch ist.

3. Verfahren nach Anspruch 2, welches weiterhin umfasst:

wenn das Hartkopieduplikat (35) authentisch ist, Kopieren des Inhalts, aber nicht der digitalen Signatur (36) auf wenigstens eine andere Hartkopie (40).

4. Prozess nach wenigstens einem der Ansprüche 1 bis 3, wobei

die digitale Signatur (36) unter Verwendung einer Zwei-Schlüssel-Authentifizierung mit einem geheimen Signierschlüssel erzeugt wird, welcher die Entität wiedergibt.

5. Verfahren nach Anspruch 4, wobei:

das authentifizierbare Hartkopieduplikat (35) weiterhin einen öffentlichen Schlüssel umfasst, der mathematisch auf den geheimen Signierschlüssel bezogen ist.

6. Einheit zum Erzeugen eines authentifizierbaren Hartkopieduplikats (35) eines Originaldokuments (20), das durch eine Entität bereitgestellt wird, wobei die Einheit umfasst:

eine Einrichtung zum Empfangen des Originaldokuments (20) von der Entität,

eine Einrichtung (64) zum Kopieren des Inhalts des Originaldokuments (20),

eine Einrichtung (50, 51) zum Empfangen von Information, welche die Identität eindeutig identifiziert,

eine Einrichtung (52) zum Verifizieren der Information,

eine Einrichtung (66, 62) zum Erzeugen einer digitalen Signatur (36), welche den Dokumenteninhalt und die Identität der Entität wiedergibt, und

eine Einrichtung (64) zum Erzeugen des Hartkopieduplikats (35), das den Dokumenteninhalt und die digitale Signatur (36) umfasst.

7. Einheit nach Anspruch 6, wobei:

die Einrichtung (62) zum Erzeugen der digitalen Signatur (36) eine Zwei-Schlüssel-Authentifizierung mit einem geheimen Signierschlüssel verwendet, welcher die Entität wiedergibt.

8. Einheit nach Anspruch 7, welche weiterhin umfasst:

eine Einrichtung zum Einfügen eines öffentlichen Schlüssels, der mathematisch auf den geheimen Signierschlüssel bezogen ist, auf dem Hartkopieduplikat (35).

9. Einheit zum Authentifizieren eines authentifizierbaren Hartkopieduplikats (35), das aus einem durch eine Entität bereitgestellten Originaldokument (20) erzeugt wird und den Inhalt des Originaldokuments (20) sowie eine digitale Signatur (36) umfasst, welche den Dokumenteninhalt und die Identität der Entität wiedergibt, wobei die Einheit umfasst:

eine Einrichtung zum Empfangen des Hartkopieduplikats (35), und

eine Einrichtung (55, 56) zum Prüfen der digitalen Signatur (36).

10. Einheit nach Anspruch 9, welche weiterhin umfasst:

eine Einrichtung (58) zum Angeben, ob das Hartkopieduplika (35) authentisch ist.

11. Einheit nach Anspruch 9 oder 10, welche weiterhin umfasst:

eine Einrichtung zum Kopieren des Dokumenteninhalts, aber nicht der digitalen Signatur (36) auf wenigstens eine andere Hartkopie (40), wenn das authentifizierbare Hartkopieduplikat (35) authentisch ist.

Revendications

1. Procédé destiné à réaliser une duplication de copie permanente authentifiable (35) d'un document original (20) fourni par une entité, comprenant :

la copie du contenu dudit document original (20) sur ladite copie permanente (35), et l'incorporation sur ladite copie permanente (35) d'une signature numérique (36) représentant ledit contenu et l'identité de ladite entité.

2. Procédé destiné à authentifier une duplication de copie permanente authentifiable (35) faite à partir d'un document original (20) fourni par une entité et comprenant le contenu dudit document original (20) et une signature numérique (36) représentant ledit contenu et l'identité de ladite entité, ledit procédé comprenant :

le contrôle de ladite signature numérique (36) sur ladite duplication de copie permanente (35), et
l'indication du fait que ladite duplication de copie permanente (35) est authentique.

3. Procédé selon la revendication 2, comprenant en outre :
si ladite duplication de copie permanente (35) est authentique, la copie dudit contenu mais non pas de ladite signature numérique (36) sur au moins une autre copie permanente (40).

4. Procédé selon les revendications 1 à 3, dans lequel :
ladite signature numérique (36) est générée en utilisant une authentification à double clé avec une clé de signature secrète représentant ladite entité.

5. Procédé selon la revendication 4, dans lequel :
ladite duplication de copie permanente authentifiable (35) comprend en outre une clé publique qui est mathématiquement liée à ladite clé de signature secrète.

6. Unité destinée à réaliser une duplication de copie permanente authentifiable (35) d'un document original (20) fourni par une entité, comprenant :

un moyen destiné à recevoir ledit document original (20) de ladite entité,
un moyen (54) destiné à copier le contenu dudit document original (20),
un moyen (50, 51) destiné à recevoir des informations identifiant de façon unique ladite entité,
un moyen (52) destiné à vérifier lesdites informations,
un moyen (59, 62) destiné à générer une signature numérique (36) représentant ledit contenu et l'identité de ladite entité, et
un moyen (64) destiné à produire ladite duplication de copie permanente (35) comprenant ledit contenu et ladite signature numérique (36).

7. Unité selon la revendication 6, dans laquelle :
ledit moyen (62) destiné à générer ladite signature numérique (36) utilise une authentification à double clé avec une clé de signature secrète représentant ladite entité.

8. Unité selon la revendication 7, comprenant en outre :
un moyen destiné à incorporer une clé publique qui est mathématiquement liée à ladite clé de signature secrète sur ladite duplication de copie permanente (35).

9. Unité destinée à authentifier une duplication de copie permanente authentifiable (35) faite à partir d'un document original (20) fourni par une entité et comprenant le contenu dudit document original (20) et une signature numérique (36) représentant ledit contenu et l'identité de ladite entité, ladite unité comprenant :

un moyen destiné à recevoir ladite duplication de copie permanente (35), et
un moyen (56, 66) destiné à contrôler ladite signature numérique (36).

10. Unité selon la revendication 9, comprenant en outre :
un moyen (68) destiné à indiquer si ladite duplication de copie permanente (35) est authentique.

11. Unité selon la revendication 9 ou 10, comprenant en outre :
un moyen destiné à copier ledit contenu mais non pas ladite signature numérique (36) sur au moins une autre copie permanente (40), si ladite duplication de copie permanente authentifiable (35) est authentique.

FIG. 1A

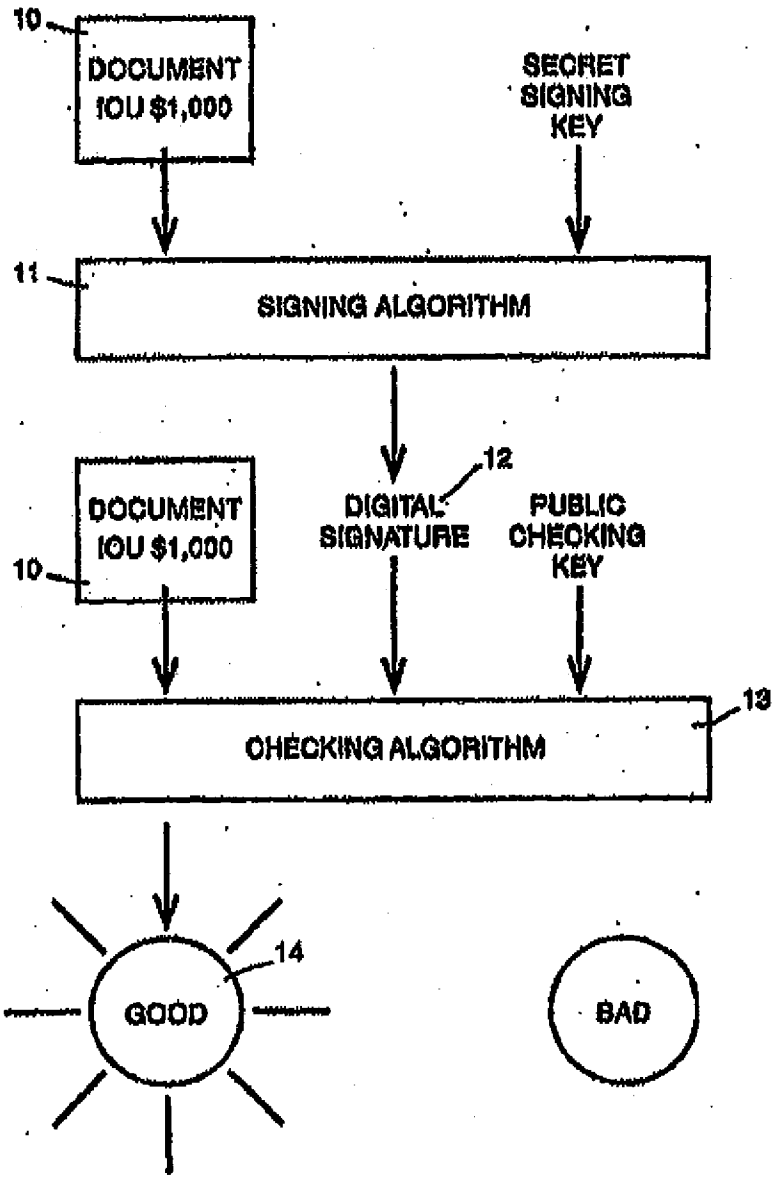
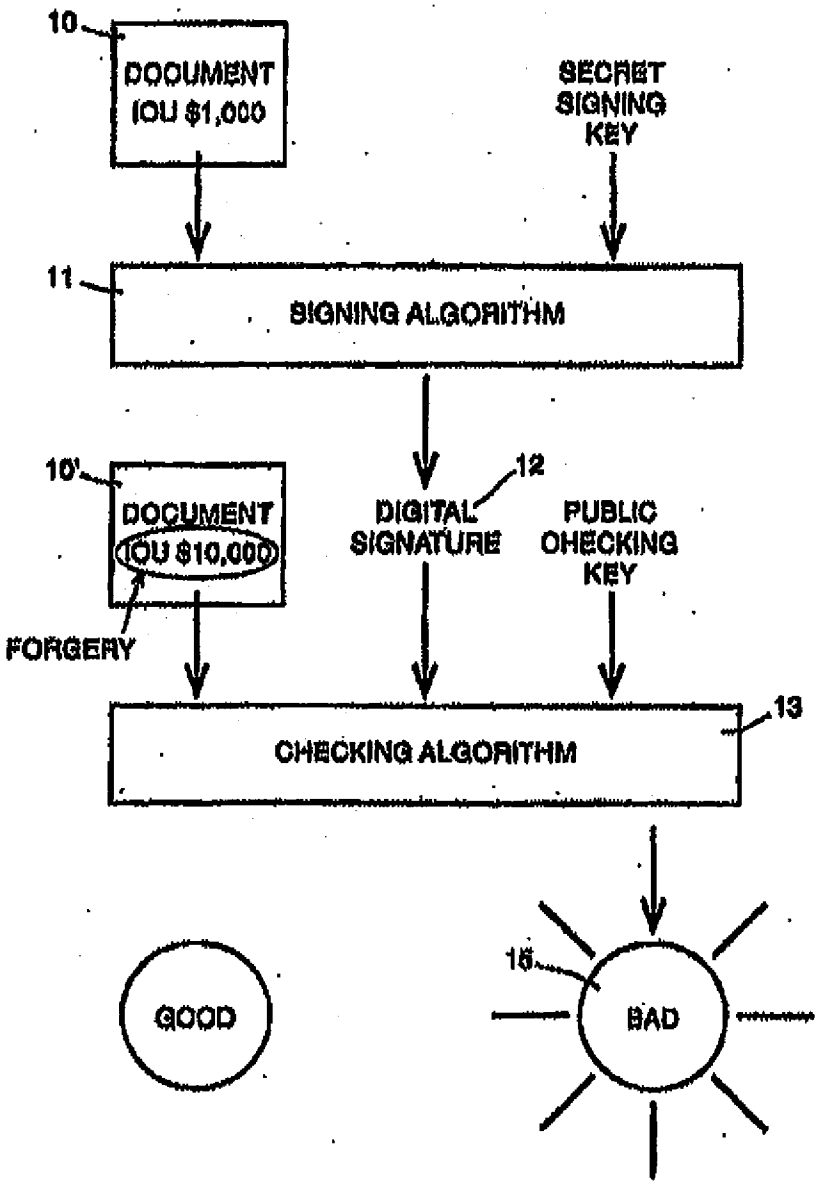

10
DOCUMENT
IOU $1,000
SECRET
SIGNING
KEY
11
SIGNING ALGORITHM
DOCUMENT
IOU $1,000
10
12
DIGITAL
SIGNATURE
PUBLIC
CHECKING
KEY
13
CHECKING ALGORITHM
14
GOOD
BAD

FIG. 1B


10
DOCUMENT
IOU $1,000
SECRET
SIGNING
KEY
11
SIGNING ALGORITHM
10'
DOCUMENT
IOU $10,000
12
DIGITAL
SIGNATURE
PUBLIC
CHECKING
KEY
FORGERY
13
CHECKING ALGORITHM
GOOD
15
BAD

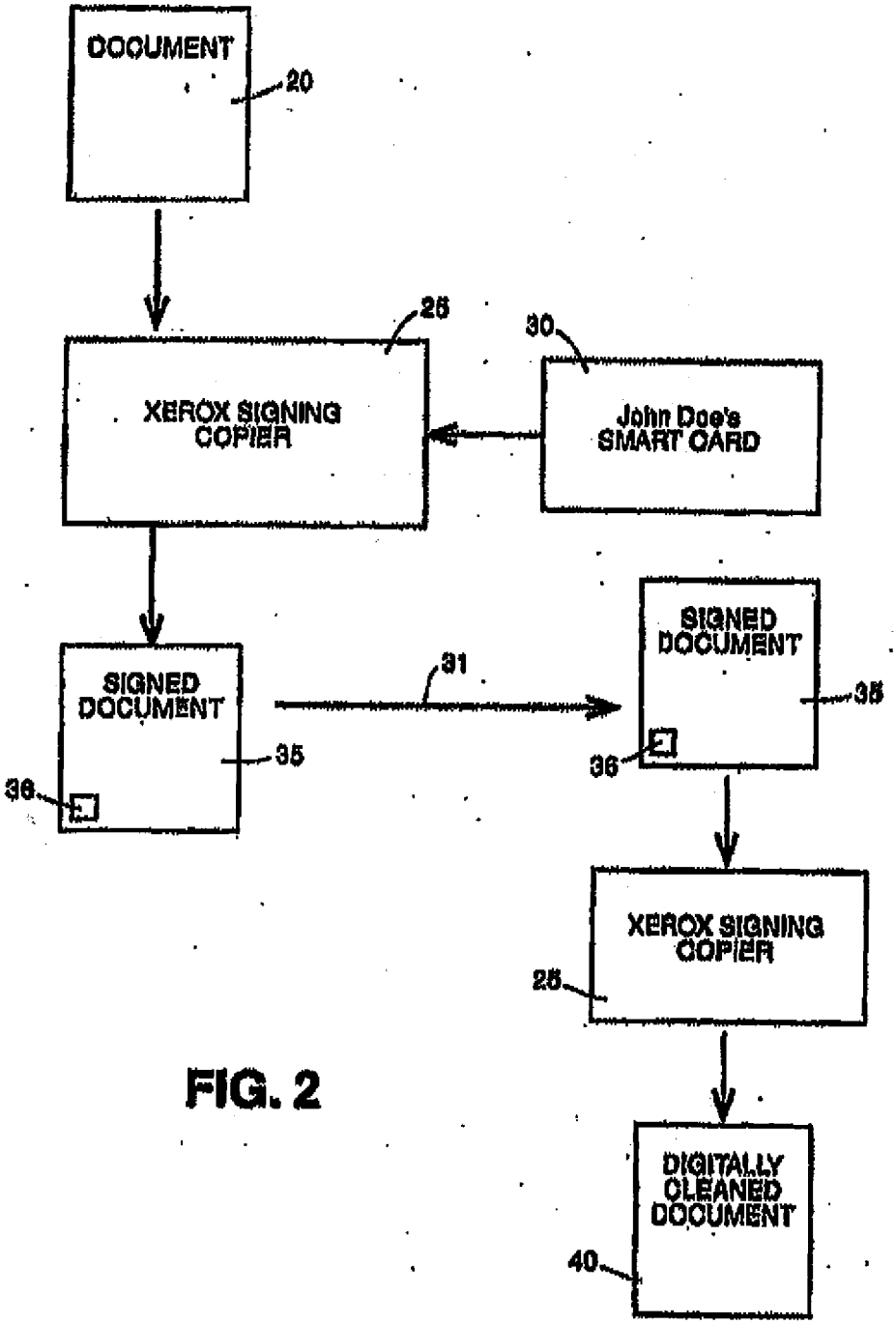
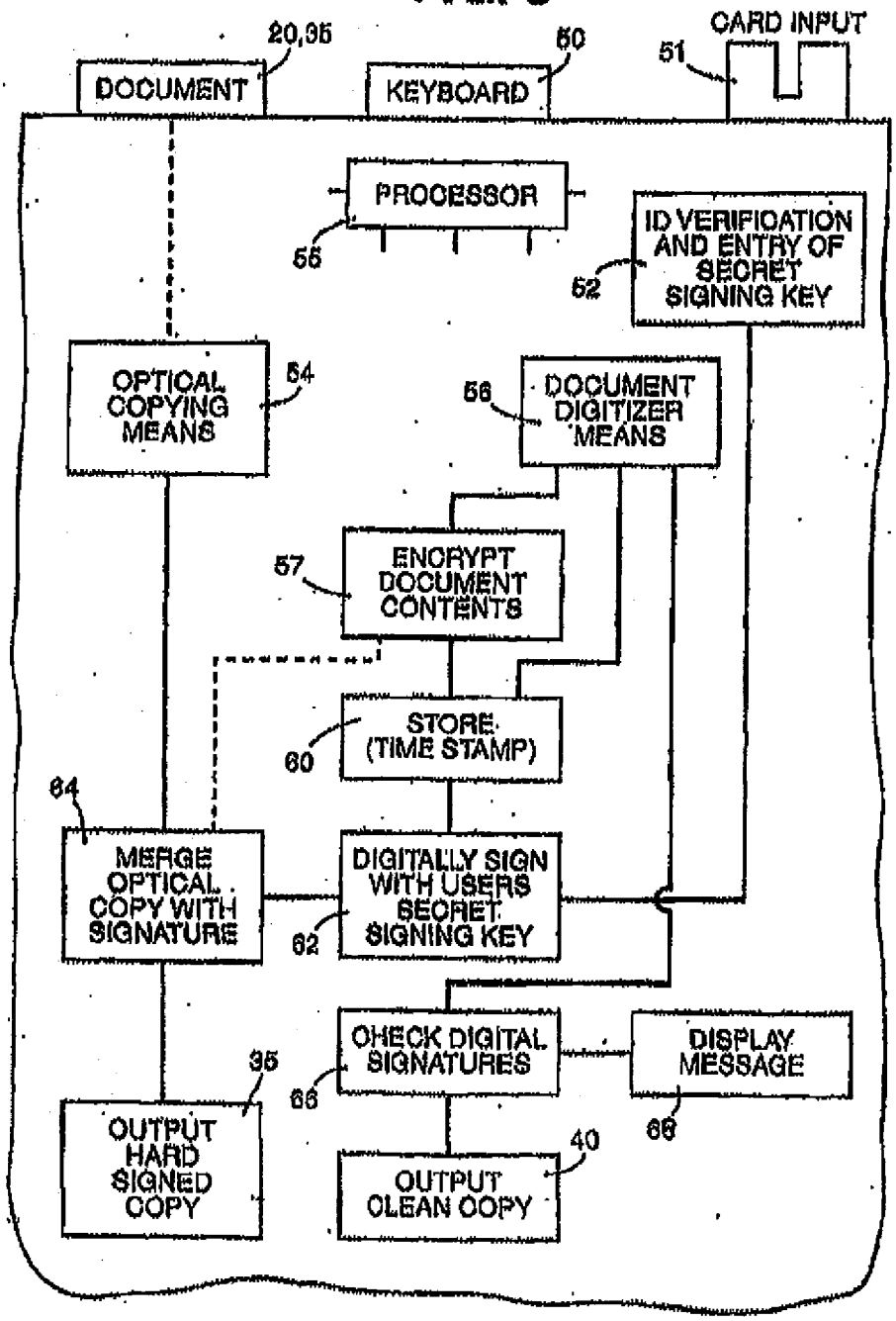

DOCUMENT
20
XEROX SIGNING COPIER
26
John Doe's SMART CARD
30
SIGNED DOCUMENT
35
36
31
SIGNED DOCUMENT
35
36
XEROX SIGNING COPIER
26
DIGITALLY CLEANED DOCUMENT
40

FIG. 2

FIG. 3


20,35
DOCUMENT
50
KEYBOARD
51
CARD INPUT
PROCESSOR
55
ID VERIFICATION AND ENTRY OF SECRET SIGNING KEY
52
OPTICAL COPYING MEANS
54
56
DOCUMENT DIGITIZER MEANS
57
ENCRYPT DOCUMENT CONTENTS
60
STORE (TIME STAMP)
64
MERGE OPTICAL COPY WITH SIGNATURE
DIGITALLY SIGN WITH USERS SECRET SIGNING KEY
62
CHECK DIGITAL SIGNATURES
66
DISPLAY MESSAGE
68
35
OUTPUT HARD SIGNED COPY
40
OUTPUT CLEAN COPY

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 727 894 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 158(3) EPC

(43) Date of publication:
21.08.1996 Bulletin 1996/34

(21) Application number: 95929249.4

(22) Date of filing: 29.08.1995

(51) Int. Cl.⁶: H04L 9/32, G09C 1/00, G06F 15/00

(86) International application number:
PCT/JP95/01708

(87) International publication number:
WO 96/07258 (07.03.1996 Gazette 1996/11)

(84) Designated Contracting States:
DE FR GB

(30) Priority: 30.08.1994 JP 227414/94

(71) Applicant: KOKUSAI DENSHIN DENWA CO., LTD
Shinjuku-ku Tokyo 163-03 (JP)

(72) Inventors:
• SUZUKI, Toshinori
Tokyo 175 (JP)
• OHASHI, Masayoshi
Saitama 355 (JP)

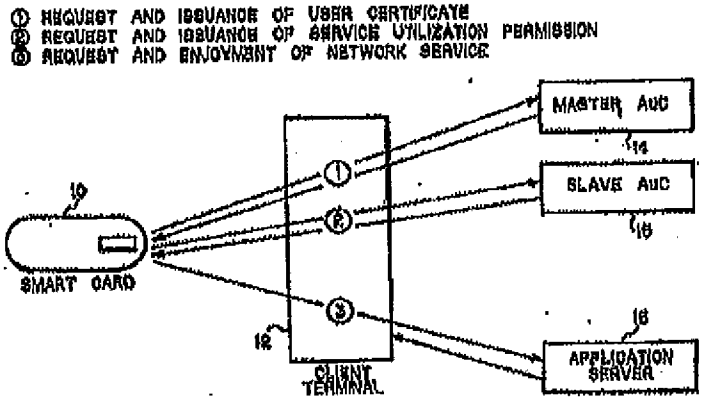
(74) Representative: de Beaumont, Michel
1bis, rue Champollion
38000 Grenoble (FR)

(54) CERTIFYING SYSTEM

(57) An authentication system whereby authentication load can be distributed in the network without sharing secret information of users is provided.

The system has a single master authentication center arranged in the network, the master authentication center sharing with the user a user secret key, and a plurality of slave authentication centers sharing with the master authentication center respective secret keys different from the user secret key. The master authentication center authenticates the user by using the user secret key and issues a certificate information which certifies legitimation of the user, to the user if the user is authenticated as a legitimate user. The slave authentication center authenticates the certificate information from the user and issues a permission information which allows an access to a specified server or an application server in the network, to the user if the user is authenticated as a legitimate user.

Fig. 2



EP 0 727 894 A1

Printed by Rank Xerox (UK) Business Services
2.13.2/4

Description

Technical Field

The present invention relates to an authentication system for identifying a user by network when the user intends to get network services.

Background Art

In order to confirm that a user who requests network services or communications (hereinafter called as a network user) is a legitimate user, it is necessary at the network side to authenticate this user.

A prover is in general identified such that;

(1) information possessed only by the prover,
(2) is identified by a verifier by means of a certain method,

where the prover is a person being authenticated and the verifier is a person authenticating.

The information possessed only by the prover (1) can be classified to the following two information of;

(1-1) information artificially provided (password, identification number, secret key, etc), and
(1-2) information based upon individual attribute (holograph, fingerprint, voiceprint, retina pattern, etc).

Authentication depending on the information based upon individual attribute (1-2) except for the holograph is now not appropriate for use in an authentication device via a network because of its low receptive capacity in society, its poor convenience, its poor identification ratio and a high manufacturing cost of the authentication apparatus. Therefore, in most cases, the information artificially provided (1-1) such as password, secret number or secret key are used as the information possessed only by the prover.

The information artificially provided (information inherent in user) can be classified, depending upon its storing way, to the following three methods of;

(1-1-1) storing information in mind of the user (password, identification number, etc),
(1-1-2) storing information in a storage possessed by the user (for general key, magnetic card, IC card, etc), and
(1-1-3) storing information by combination of (1-1-1) and (1-1-2) (cash dispenser provided in a banking organ, etc).

Since the above classification is performed from a standpoint of an authentication system, a case wherein the user takes a note of his password or identification number to his memorandum will be classified to (1-1-1).

In a computer network, the above-mentioned method of storing information in mind of the user (1-1-1) is mainly utilized. However, according to this storing method (1-1-1), impersonation can be relatively easily performed by decoding or stealing the password or identification number and also, in most cases, this impersonation will not be found out by the person himself until he practically suffers damage. This is because the secret information according to this method (1-1-1) itself may be directly revealed, and thus leakage, stealing or wiretap of the password or of the identification number will be easily succeeded without consciousness of the user.

Contrary to this, according to the method of storing information in a storage possessed by the user (1-1-2), since the user can found out loss or stealing of his possessed storage and thus possible damage can be foreknown, the damage can be prevented from occurring by performing an adequate procedure against the loss or stealing. The storing method (1-1-3) combined by (1-1-1) and (1-1-2) will be effective so as to prevent illegally even if the possessed storage is stolen. Of course, however, the damage will not be prevented from occurring if the storage is forged without consciousness of the network and the user. Therefore, it is desired to use a storage which is difficult to forge. For this aim, an IC card with CPU (herein after called as a smart card) which will keep high confidentiality is the optimum.

The method of identifying by the verifier (2) can be substantially classified, depending upon what kind of information does the prover present to the verifier (network), to the following two methods of;

(2-1) presenting user's inherent information as it is, and
(2-2) presenting a calculation result of the user's inherent information.

However, the method of presenting user's inherent information (2-1) has disadvantage of easily revealing his secret inherent information. In particular, if this method is combined with the aforementioned method of storing information in mind of user (1-1-1), there may be extremely dangerous for revealing the secret inherent information to public. The method of presenting a calculation result of the user's inherent information (2-2) may be classified in accordance with kinds of this calculation.

Anyway, the present invention relates to an authentication method of sharing secret user's inherent information between a prover (user) and a verifier (network), encrypting and decrypting the information at the user and the network, respectively, and then checking identification of the decrypted information with the shared information so as to verify the user.

It should be noted that it is difficult to combine the method of presenting a calculation result of the user's inherent information (2-2) with the authentication

method using the information based upon individual attribute (1-2).

As is described above, the combination of the storing method (1-1-1) with the method of presenting user's inherent information (2-1) is the most dangerous, and the combination of the storing method (1-1-3) with the method of presenting a calculation result of the user's inherent information (2-2) is the safest. An authentication system using this latter combined method with smart cards is now realized in a part of mobile communication networks such as GSM (Global System for Mobile communications).

However, according to the system using the method of presenting a calculation result of the user's inherent information (2-2), since the decryption calculation has to be performed at every authentication process, load of the authentication process will be concentrated to an authentication device in the network, which manages secret information of users.

In order to avoid such problem, load of the calculations for authentication can be distributed in a plurality of authentication devices by providing the secret information of users to them. However, dispersing the secret information of users to the plurality of the authentication devices will result not only lowered safety of authentication but also extremely increased cost for managing and for operating the secret information in safe.

Disclosure of Invention

It is therefore an object of the present invention to provide an authentication system whereby authentication load can be distributed in the network without sharing secret information of users when each of the users is verified.

According to the present invention, an authentication system adopting an authentication scheme for verifying a user from a network, by sharing the same secret key between the user and the network, encrypting a known information using the secret key at the user to produce first encrypted information, transmitting the first encrypted information from the user to the network, encrypting the known information using the secret key at the network to produce second encrypted information, and collating the transmitted first encrypted information with the produced second encrypted information at the network, is provided. The system has a single master authentication center arranged in the network, the master authentication center sharing with the user a user secret key, and a plurality of slave authentication centers sharing with the master authentication center respective secret keys different from the user secret key. The master authentication center authenticates the user by using the user secret key and issues a certificate information which certifies legitimation of the user, to the user if the user is authenticated as a legitimate user. The slave authentication center authenticates the certificate information from the user and issues a permission information which allows an access to a specified server or an application server in the network, to the user if the user is authenticated as a legitimate user.

As will be apparent from the above description, only one master authentication center possesses the user secret keys other than the respective users, and therefore each of the user secret keys is not shared by a plurality of users. Furthermore, since the master authentication center authenticates the user by using the user secret key and issues a certificate information which certifies legitimation of the user and the slave authentication center authenticates the certificate information from the user and issues a permission information which allows an access to a specified server or an application server in the network, authentication load can be distributed.

The application server can execute the role of the above-mentioned slave authentication center. In this case, the permission information and also the slave authentication center can be omitted.

It is preferred that the system adopts an authentication scheme not only for verifying a user from a network, by sharing the same secret key between the user and the network, encrypting a known information using the secret key at the user to produce first encrypted information, transmitting the first encrypted information from the user to the network, encrypting the known information using the secret key at the network to produce second encrypted information, and collating the transmitted first encrypted information with the produced second encrypted information at the network, but also for verifying the network from the user, by encrypting a known information using the secret key at the network to produce third encrypted information, transmitting the third encrypted information from the network to the user, encrypting the known information using the secret key at the user to produce fourth encrypted information, and collating the transmitted third encrypted information with the produced fourth encrypted information at the user. This mutual authentication can improve security and certainty of authentication.

It is also preferred that the user has an IC card provided with a CPU (smart card), and that the smart card executes management of the user secret key and encryption and decryption of the information. By using such a smart card for managing a user secret key and for encrypting information, the secret key will not reveal to a client terminal and therefore forgery thereof will become quite difficult resulting to keep higher security of authentication.

Preferably, the secret key used for encrypting the known information is a key using a random number generated at the user. Encryption using this key with a random number will provides more highly security.

Brief Description of Drawings

Fig. 1 is a block diagram schematically showing a constitution of an embodiment (first embodiment) of

an authentication system according to the present invention;

Fig. 2 is a sketch schematically showing three phase sequence of authentication processes in the embodiment shown in Fig. 1;

Fig. 3 is a sketch showing detail procedure in a first authentication phase shown in Fig. 2;

Fig. 4 is a sketch showing detail procedure in a second authentication phase shown in Fig. 2;

Fig. 5 is a sketch showing detail procedure in a third authentication phase shown in Fig. 2;

Fig. 6 is a block diagram schematically showing a constitution of an another embodiment (second embodiment) of an authentication system according to the present invention;

Fig. 7 is a sketch showing detail procedure in a first phase of an example of authentication processes in the embodiment shown in Fig. 6;

Fig. 8 is a sketch showing detail procedure in a second phase of the example of the authentication processes in the embodiment shown in Fig. 6;

Fig. 9 is a sketch showing detail procedure in a first phase of an another example of authentication processes in the embodiment shown in Fig. 6;

Fig. 10 is a sketch showing detail procedure in a second phase of the another example of the authentication processes in the embodiment shown in Fig. 6; and

Fig. 11 is a sketch showing content of a certification used in the authentication processes in the embodiment shown in Fig. 6.

Best Mode for Carrying Out the Invention

Referring to drawings, embodiments according to the present invention will be described in detail.

First Embodiment

Fig. 1 is a block diagram schematically showing a constitution of an embodiment of an authentication system according to the present invention.

This embodiment utilizes the already mentioned method of presenting the calculation result of user's inherent information (2-2) and also the already mentioned method of storing the user's inherent information in a smart card (1-1-2). According to the present invention, however, the method of storing the user's information in mind of the user (1-1-1) or the storing method (1-1-3) of combination of (1-1-1) and (1-1-2) may be utilized. It is not easy and will result to reveal the secret information to perform the calculation of the method (2-2) by the user himself. Thus, this calculation should be done by a possession of the user, having both storing and calculation functions, such as a smart card instead of the user himself. In this case, the above-mentioned storing methods (1-1-2) and (1-1-3) are used.

In Fig. 1, reference numeral 10 denotes a smart card provided with program and file which will be described later and possessed by each user, 11 denotes a card reader/writer for reading information from or writing information to the smart card 10, and 12 denotes a client terminal connected to the reader/writer 11, provided with client side application and authentication kernel, respectively. The reader/writer 11 will be mounted inside or outside of the client terminal 12.

The smart card 10 is constituted by an IC card with arithmetic function, which consists of a memory having a capacity of for example about 16 KB and a CPU of for example 8 bits. The client terminal 12 is constituted by a general purpose work station or a general purpose personal computer and connected to a network 13 such as for example LAN via a communication line. This client terminal 12 is an access point of the user to the network 13 and also a terminal for providing network service from an application server side. Although only one client terminal 12 is illustrated in Fig. 1, in fact there may be a plurality of client terminals having the similar constitution as the terminal 12 and connected via respective communication lines.

A single master authentication center (master AuC) 14 provided with authentication program which will be described later, a plurality of slave authentication centers (slave AuCs) 15 provided with authentication program which will be described later, and at least one application server (APS) 16 provided with server side application and authentication kernel are connected to the network 13 so as to be able to communicate with the client terminal 12 via this network 13.

In a database 14a provided for the master authentication center 14, the least of user data such as user's secret keys, system log, black list of the users and slave AuC data such as secret keys of the respective slave authentication centers 15 are stored. In a database 15a provided for the slave authentication center 15, the least of APS data such as secret key(s) of the application server(s) 16 are stored. The master authentication center 14, the slave authentication center 15 and the application server 16 are constituted by general purpose work stations, respectively. Communications between the general purpose work stations and between the general purpose work station and the general purpose personal computer are carried out through RPC (Remote Procedure Call).

The memory in the smart card 10 stores a secret key inherent in a smart cardholder (user secret key Ku). The CPU in the smart card 10 is programed so as to calculate a cryptographic function f with this secret key Ku.

The network 13 has the only one master authentication center 14, and the user secret key Ku is held only by this master authentication center 14. Both this single master authentication center 14 and the slave authentication centers 15 together have respective secret information inherent in the respective slave authentication centers 15 (slave AuC secret keys Kat, Ka2, Ka3,...). Also, both the application servers 16 for providing network services to the users and the slave authentication centers 15 together have secret information inherent in

every application servers 16 (APS secret keys Ka1, Ka2, Kas,...).

Authentication processes in this embodiment will now be described. In the following processes, suppose that a user intends to enjoy a desired network service from a specific application server 16.

First, the user inserts his possessing smart card 10 into the reader/writer 11 and then accesses the client terminal 12 as follows so as to activate the smart card 10.

For the card user, a PIN (Personal Identification Number) code has been previously defined, and this defined PIN code has been stored in the smart card 10. The user inputs his PIN code through the client terminal 12 into the smart card 10 so that coincidence between the input PIN code and one stored in the smart card 10 is checked. This check of the PIN code is executed by internal operation of the smart card 10. If PIN code input is successively failed three times, no more access of user capability is possible. Since the memory in the smart card 10 is a nonvolatile storage, the number of the past successive PIN input failure will be held even if the power is off.

After the smart card 10 is activated by local verification between the user and the smart card 10, authentication processes are carried out with three phase sequence schematically shown in Fig. 2.

A first phase is ① request and issuance of a user certificate. In this first phase, the user side (smart card 10) requests the master AuC 14 to issue a certification information (user certificate) used for executing authentication procedure with the slave AuC 15. The issued user certificate which has a valid period is stored in the smart card 10. Prior to accessing the master AuC 14, the user side (smart card 10 or client terminal 12) confirms the validity of the already obtained user certificate. As long as the user certificate is valid, the authentication processes can be jumped to a next second phase without accessing the master AuC 14. This causes throughput in the master AuC 14 to decrease.

The second phase is ② request and issuance of a service utilization license. In this second phase, the user side (smart card 10) requests, with indicating the user certificate, the slave AuC 15 to issue a permission information (service utilization license) for utilizing the application server 16. The slave AuC 15 will verify the User Certification presented by the smart card 10, and issue the service utilization permission if verified.

A third phase is ③ request and enjoyment of a network service. In this third phase, the user side (smart card 10) requests, with indicating the service utilization license, the application server 16 to provide a desired network service. The application server 16 will verify the indicated service utilization license and provide the requested service to the client terminal 12 if the indicated license is verified.

Referring to Figs. 3, 4 and 5 which show detail procedure in the above-mentioned respective authentication phases, each procedure will be described in detail. Symbols illustrated in these figures indicate as follows.

AuC	authentication center
IDu	inherent number assigned to a smart card (held by the smart card and the master AuC only)
Ku	user secret key (held by the smart card and the master AuC only)
Ks	slave AuC secret key (shared by the master AuC and each of the slave AuCs only)
Ka	APS secret key (shared by slave AuC and each of the APSs only)
Ku-s	secret key between the smart card and the slave AuC (disposable key generated by master AuC at every issuance of User Certificate)
Ku-a	secret key between the smart card and the APS (disposable key generated by slave AuC at every issuance of Service Utilization License)
c_addr	network address of the client terminal
Ts	time stamp (indicating current time or expiring time of valid period)
Cert	user certificate (issued by the master AuC and decrypted only by the slave AuC)
Lic	service utilization license (issued by the slave AuC and decrypted only by the APS)
A/Res	access/response message
|	process of concatenating data with each other
X=Y?	process of confirming coincidence of time stamps X and Y within a predetermined margin
f(data,K)	process of encrypting data with key K
f^{-1}(data,K)	process of decrypting or inversely encrypting data with K

Fig. 3 illustrates procedure in the first phase ① for requesting and issuing a user certificate. As shown in this figure, at first, the client terminal 12 generates a time stamp Ts1 indicating the current time. The generated time stamp Ts1 and a network address c_addr of this client terminal 12 are transmitted to the smart card 10. In Fig. 3, this transmission is represented by [Ts1,c_addr]. These transmitted data are concatenated with each other in the smart card 10, and then the concatenated data is encrypted by using a user secret key Ku previously stored in the smart card 10 to obtain A=f(Ts1|c addr,Ku). Then, an inherent card number IDu stored in this smart card 10 is read out and transmitted to the master AuC 14 with the encrypted A as for an authentication request. This transmission is represented by [IDu,A] in Fig. 3. The card number IDu is

transmitted without encryption. Although all communications between the smart card 10 and the master AuC 14 are executed through the client terminal 12, this client terminal 12 itself cannot analyze the encrypted data.

The master AuC 14 generates a time stamp Ts2 indicating a time of receiving the authentication request from the client terminal 12. Then, a user secret key Ku is inquired from the received card number IDu using the database 14a. Then, the encrypted A is decrypted by means of a function Ts1|c_addr=f^{-1}(A,Ku) with the inquired user secret key Ku to obtain the time stamp Ts1 of the client terminal 12 and the network address c_addr. Coincidence between the obtained time stamp Ts1 and the time stamp Ts2 generated at the master AuC 14 is then verified. Since Ts2 is necessarily delayed from Ts1, this collation of coincidence has to be considered with a margin of time delay of for example ten seconds. If the user secret key Ku used in encryption at the smart card side to produce A is incorrect key, the decrypted Ts1 will extremely differ from Ts2. Thus, if the decrypted Ts1 does not coincide with Ts2 with consideration of the margin, failure of the authentication is informed to the user side and the process is terminated.

If the decrypted Ts1 coincides with Ts2 with consideration of the margin, following procedure for issuing a user certificate will be executed. First, at the master AuC 14, a secret key between the smart card 10 and the slave AuC 15 Ku-s is generated and then an original user certificate Cert(Ku-s,Ts2,c_addr) consisting of Ku-s, Ts2 and c_addr. This user certificate Cert is encrypted using a slave AuC secret key Ks which is shared only by the master AuC and its slave AuC, to produce Cert'. Namely, by using a cryptographic function f, Cert' is obtained from Cert=f(Cert,Ku).

Thereafter, Res is generated by inversely encrypting Cert' as well as Ts2 and Ku-s using the user secret key Ku, namely from Res=f^{-1}(Cert'|Ts2|Ku-s,Ku). The generated Res is then returned to the smart card 10 as a response message with respect to the access from the user (Res). Because of lower calculation capacity, it is desired that the smart card 10 executes only calculation based upon encryption function f. Thus, at the master AuC 14, inverse encryption f^{-1} is executed instead of encryption f.

When the smart card 10 receives the response message Res, the received Res is decoded by the function f using the user secret key Ku, namely from Cert'|Ts2|Ku-s=f(Res,Ku), to extract and store into the memory in the smart card 10 the encrypted user certificate Cert', the time stamp Ts2 and the secret key Ku-s. The extracted time stamp Ts2 is transmitted to the client terminal 12 and therein verified, with respect to coincidence, with the time stamp Ts1 which was generated at this terminal 12 (Ts1=Ts2?). Thus, the master AuC 14 is verified by the smart card 10 resulting that the smart card 10 and the master AuC 14 are mutually authenticated each other. According to the above-mentioned mechanism, the secret key between the smart card and the slave AuC Ku-s is used for communication between the smart card 10 and the slave AuC 15 without being revealed outside the smart card 10. Since Cert' is encrypted using the slave AuC secret key Ks, the smart card 10 and the client terminal 12 cannot analyze it at all.

At a next authentication procedure, prior to accessing the master AuC 14, the client terminal 12 read out the time stamp Ts2 stored in the smart card 10 and compares it with the current time to confirm the validity of the stored user certificate Cert'. As long as the user certificate is valid, the authentication processes can be jumped the first phase shown in Fig. 3 to the next second phase without accessing the master AuC 14 causing throughput in the master AuC 14 to decrease.

Fig. 4 illustrates procedure in the second phase ② for requesting and issuing a service utilization license. As shown in this figure, at first, the client terminal 12 generates a time stamp Ts3 indicating the current time. The generated time stamp Ts3 and a network address c_addr of this client terminal 12 are transmitted to the smart card 10. In Fig. 4, this transmission is represented by [Ts3,c_addr]. If this second phase is executed just after the first phase, as Ts3 is equal to Ts1 with consideration of the margin and c_addr has already been sent, this process can be omitted. These transmitted data are concatenated with each other in the smart card 10, and then the concatenated data is encrypted by using the secret key Ku-s which was transmitted from the master AuC 14 with the user certificate Cert' and stored in the smart card 10, to obtain A'=f(Ts3|c_addr,Ku-s). Then, the user certificate Cert' is transmitted to the slave AuC 15 with the encrypted A'. This transmission is represented by [Cert',A] in Fig. 4. Although all communications between the smart card 10 and the slave AuC 15 are also executed through the client terminal 12, this client terminal 12 itself cannot analyze the encrypted data.

The slave AuC 14 generates a time stamp Ts4 indicating a time of receiving the access from the client terminal 12. Then, the encrypted user certificate Cert' is decrypted by means of a function Cert=f^{-1}(Cert',Ks) using the slave AuC secret key Ks stored in the slave AuC 15 to obtain a decrypted Cert. In this decrypted user certificate Cert, the time stamp Ts2 indicating the issuance time of this user certificate Cert, the secret key Ku-s and the network address of the client terminal 12 c_addr are included. Then, the obtained time stamp Ts2 is checked by the time stamp Ts4 to confirm that the user certificate Cert was issued at a time within a predetermined period from now. Thus, validity of this user certificate Cert is confirmed.

Then, the encrypted A' is decrypted by means of a function Ts3|c_addr=f^{-1}(A',Ku-s) with the secret key Ku-s contained in the user certificate Cert to obtain the time stamp Ts3 of the client terminal 12 and the network address c_addr.

Coincidence between the obtained time stamp Ts3 and the time stamp Ts4 generated at the slave AuC 15, and coincidence between c_addr contained in the user

certificate Cert and c_addr contained in A' are then verified. If the user certificate Cert is forged one, since the secret key Ku-s and the network address c_addr contained in this Cert cannot be extracted and also the decryption using this key Ku-s cannot be executed, the collation will be failed. Thus, in this case, the slave AuC 15 will not issue a service utilization license Lic and failure of the authentication is informed to the user side to terminate the process.

If the collation succeeds, following procedure for issuing a service utilization license Lic will be executed. First, at the slave AuC 15, a secret key between the smart card 10 and a specific application server 16 Ku-a is generated and then an original service utilization license Lic(Ku-a,Ts4,c_addr) consisting of Ku-a, Ts4 and c_addr. This service license Lic is encrypted using an APS secret key Ka which is shared only by the slave AuC and the specific application server, to produce Lic'. Namely, by using a cryptographic function f, Lic' is obtained from Lic'=f(Lic,Ka). This encrypted service license Lic' can be analyzed only by the specific application server having the secret key Ka.

Thereafter, Res' is generated by inversely encrypting Lic' as well as Ts4 and Ku-a using the secret key Ku-s, namely from Res'=f^{-1}(Lic'|Ts4|Ku-a,Ku-s). The generated Res' is then returned to the smart card 10 as a response message with respect to the access from the user ((Res')).

When the smart card 10 receives the response message Res', the received Res' is decoded by the function f using the secret key Ku-s, namely from Lic'|Ts4|Ku-a=f(Res',Ku-s), to extract and store into the memory in the smart card 10 the encrypted service utilization license Lic', the time stamp Ts4 and the secret key Ku-a. The extracted time stamp Ts4 is transmitted to the client terminal 12 and therein verified, with respect to coincidence, with the time stamp Ts3 which was generated at this terminal 12 (Ts3=Ts4?). Thus, the slave AuC 15 is verified by the smart card 10 resulting that the smart card 10 and the slave AuC 15 are mutually authenticated each other. According to the above-mentioned mechanism, the secret key between the smart card and the application server Ku-a is used for communication between the smart card 10 and the application server 16 without being revealed outside the smart card 10. Since Lic' is encrypted using the secret key Ka, the smart card 10 and the client terminal 12 cannot analyze it at all.

Fig. 5 illustrates procedure in the third phase ③ for requesting and enjoying a network service. As shown in this figure, at first, the client terminal 12 generates a time stamp Ts5 indicating the current time. The generated time stamp Ts5 and a network address c_addr of this client terminal 12 are transmitted to the smart card 10. In Fig. 5, this transmission is represented by [Ts5,c_addr]. If this third phase is executed just after the second phase, as Ts5 is equal to Ts3 with consideration of the margin and c_addr has already been sent, this process can be omitted. These transmitted data are concatenated with each other in the smart card 10, and then the concatenated data is encrypted by using the secret key Ku-a which was transmitted from the slave AuC 15 with the service utilization license Lic' and stored in the smart card 10, to obtain A''=f(Ts5|c_addr,Ku-a). Then, the service license Lic' is transmitted to the application server 16 with the encrypted A''. This transmission is represented by [Lic',A''] in Fig. 5. Although all communications between the smart card 10 and the application server 16 are also executed through the client terminal 12, this client terminal 12 itself cannot analyze the encrypted data.

The application server 16 generates a time stamp Ts6 indicating a time of receiving the access from the client terminal 12. Then, the encrypted service utilization license Lic' is decrypted by means of a function Lic=f^{-1}(Lic',Ka) using the APS secret key Ka stored in the application server 16 to obtain a decrypted Lic. In this decrypted service utilization license Lic, the time stamp Ts4 indicating the issuance time of this license Lic, the secret key Ku-a and the network address of the client terminal 12 c_addr are included. Then, the obtained time stamp Ts4 is checked by the time stamp Ts6 to confirm that the license Lic was issued at a time within a predetermined period from now. Thus, validity of this license Lic is confirmed.

Then, the encrypted A'' is decrypted by means of a function Ts5|c_addr=f^{-1}(A'',Ku-a) with the secret key Ku-a contained in the license Lic to obtain the time stamp Ts5 of the client terminal 12 and the network address c_addr.

Coincidence between the obtained time stamp Ts5 and the time stamp Ts6 generated at the application server 16, and coincidence between c_addr contained in the license Lic and c_addr contained in A'' are then verified. If the service utilization license Lic is forged one, since the secret key Ku-a and the network address c_addr contained in this license Lic cannot be extracted and also the decryption using this key Ku-a cannot be executed, the collation will be failed. Thus, in this case, the application server 16 will not provide a network service and failure of the authentication is informed to the user side to terminate the process.

If the collation succeeds, at the application server 16, Res'' is generated by inversely encrypting Ts6 using the secret key Ku-a, namely from Res''=f^{-1}(Ts6,Ku-a). The generated Res'' is then returned to the smart card 10 as a response message with respect to the access from the user ((Res')).

When the smart card 10 receives the response message Res'', the received Res'' is decoded by the function f using the secret key Ku-a, namely from Ts6=f(Res'',Ku-a), to extract and store into the memory in the smart card 10 the encrypted time stamp Ts6. The extracted time stamp Ts6 is transmitted to the client terminal 12 and therein verified, with respect to coincidence, with the time stamp Ts5 which was generated at this terminal 12 (Ts5=Ts6?). Thus, the application server 16 is verified by the smart card 10 resulting that

the smart card 10 and the application server 16 are mutually authenticated each other. If the mutual authentication succeeds, the application server provides the network service to the client terminal 12.

The above-mentioned authentication procedure is necessary for time synchronization between the master AuC 14, the slave AuC 15, the application server 16 and the client terminal 12. This is because a time information (time stamp) is used for an authentication data (data for cryptographic function) known by both the prover and the verifier. Instead of the time information, a random number generated at the verifier (network side) and transmitted to the user side can be utilized as an authentication data, like a challenge-response authentication protocol used in GSM. A second embodiment according to the present invention, which will be described later, uses this protocol.

In the aforementioned first embodiment, the information to be transmitted from the smart card 10 is encrypted directly using the user secret key Ku, the slave AuC secret key Ks or the APS secret key Ka. However, if a key is produced by encrypting a random number R generated at the smart card 10 using the user secret key Ku, the slave AuC secret key Ks or the APS secret key Ka and the information to be transmitted from the smart card 10 is encrypted using this produced encrypted key, higher security can be expected. In this case, the random number R has to also be transmitted to the master AuC 14, the slave AuC 15 or the application server 16.

Furthermore, although in the aforementioned embodiment, individual slave AuC keys Ks are provided for the respective slave AuCs, a single slave AuC key Ks can be shared by all the slave AuCs. In the latter case, however, security will be somewhat lowered.

Second Embodiment

Fig. 6 is a block diagram schematically showing a constitution of an another embodiment of an authentication system according to the present invention.

In the figure, reference numeral 10 denotes a smart card provided with program and file which will be described later and possessed by each user, 11 denotes a card reader/writer for reading information from or writing information to the smart card 10, and 12 denotes a client terminal connected to the reader/writer 11, provided with client side application and authentication kernel, respectively. The reader/writer 11 will be mounted inside or outside of the client terminal 12.

The smart card 10 in this embodiment is constituted by an IC card with arithmetic function, which consists of a memory having a capacity of for example equal to or less than 8 KB and a CPU of for example 8 bits. As having a simpler constitution of this embodiment than that of the first embodiment, the smart card 10 in this embodiment has the smaller capacity memory. The client terminal 12 is constituted by a general purpose work station or a general purpose personal computer and connected to a network 13 such as for example LAN via a communication line. This client terminal 12 is an access point of the user to the network 13 and also a terminal for providing network service from an application server side. Although only one client terminal 12 is illustrated in Fig. 6, in fact there may be a plurality of client terminals having the similar constitution as the terminal 12 and connected via respective communication lines.

An authentication center (AuC) 17 provided with authentication program for verifying the user and at least one application server (APS) 16 provided with server side application for providing services to the user are connected to the network 13 so as to be able to communicate with the client terminal 12 via this network 13.

In a database 17a provided for the authentication center 17, the kind of user data such as user's secret keys, system log, black list of the users and secret key(s) of the application server(s) 16 are stored. The authentication center 17 and the application server 16 are constituted by general purpose work stations, respectively. Communications between the general purpose work stations and between the general purpose work station and the general purpose personal computer are carried out through RPC (Remote Procedure Call).

The memory in the smart card 10 stores a secret key inherent in a smart card holder (user secret key Ku). The CPU in the smart card 10 is programed so as to calculate a cryptographic function f with this secret key Ku.

In the network 13, the user secret key Ku is held only by the authentication center 17.

Both this authentication center 17 and the application servers 16 together have respective secret information inherent in the respective application servers 16 (APS secret keys Ka1, Ka2, Ka3,...).

Authentication processes in this embodiment will now be described. In the following processes, suppose that a user intends to enjoy a desired network service from a specific application server 16.

First, the user inserts his possessing smart card 10 into the reader/writer 11 and then accesses the client terminal 12 as follows so as to activate the smart card 10.

For the card user, a PIN code has been previously defined, and this defined PIN code has been stored in the smart card 10. The user inputs his PIN code through the client terminal 12 into the smart card 10 so that coincidence between the input PIN code and one stored in the smart card 10 is checked. This check of the PIN code is executed by internal operation of the smart card 10. If PIN code input is successively failed three times, the smart card 10 permits no more access and thus the authentication procedure terminates. Since the memory in the smart card 10 is a nonvolatile storage, the number of the past successive PIN input failure will be held even if the power is off. This storage will be cleared if PIN

code check is succeeded within successive three times inputs.

After the smart card 10 is activated by local verification between the user and the smart card 10, authentication processes are carried out with following two phase sequence.

A first phase is request and issuance of a user certificate. In this first phase, the user side (smart card 10) requests the AuC 17 to issue a certification information (user certificate) which verifies him. The issued user certificate which has a valid period is stored in the smart card 10. Prior to accessing the AuC 17, the user side (smart card 10 or client terminal 12) confirms the validity of the already obtained user certificate. As long as the user certificate is valid, the authentication processes can be jumped to a next second phase without accessing the AuC 17. This causes throughput in the AuC 17 to decrease.

The second phase is request and enjoyment of a network service. In this phase, the user side (smart card 10) requests, with indicating the user certificate, the application server 16 to provide a desired network service. The application server 16 will verify the indicated user certificate and provide the requested service to the client terminal 12 if the indicated certificate is verified.

Figs. 7 and 8 show an example of detail procedure in the above-mentioned respective authentication phases. Figs. 9 and 10 show an another example of detail procedure wherein a mutual-authentication mechanism is adopted. Combination of procedure of Fig. 7 and that of Fig. 10, and combination of procedure of Fig. 9 and that of Fig. 8 can be possible.

Fig. 7 illustrates procedure in the first phase for requesting and issuing a user certificate. As shown in this figure, at first, an inherent card number IDu stored in this smart card 10 is read out and transmitted to the AuC 17 with a name of the application server APS NAME which will provide a desired network service as an authentication request. This transmission is represented by [IDu,APS NAME] in Fig. 7. The card number IDu and the APS NAME are transmitted without encryption. The APS NAME will be referred when a user certificate Cert and an authentication information AuInfo are issued later.

The AuC 17 generates a random number Rnd and transmits it (called a challenge) to the smart card 10. The smart card 10 then encrypts the received random number Rnd using the user secret key Ku stored in its memory to generate a response Res by means of a function Res=f(Rnd,Ku). The generated response Res is returned to the AuC 17. The AuC 17 inquires the user secret key Ku from the received card number IDu using the database 17a, and then, executes the same encryption of the random number Rnd as done in the smart card 10 using the user secret key Ku to generate Res' by means of a function Res'=f(Rnd,Ku). The generated Res' is then compared with the response Res transmitted from the smart card 10. If the user is a legitimate user and the user secret key Ku is correct one, Res will coincides with Res'. However, if the user secret key Ku is incorrect, the calculated results Res and Res' will not coincide with each other. In this case, failure of the authentication is informed to the user side and the process is terminated.

If the encrypted Res' coincides with Res, a user certificate Cert and an authentication information AuInfo are issued for the smart card 10. Contents of the issued user certificate Cert and authentication information AuInfo are indicated in Fig. 11 as an example.

In order to prevent from fraudulent, the user certificate Cert is encrypted using an APS secret key Ka which is shared only by the AuC 17 and the APS 16 corresponding to the application server name APS NAME, to produce Cert'. Namely, by using a cryptographic function f, Cert' is obtained from Cert'=f(Cert,Ka). The authentication information AuInfo and the encrypted user certificate Cert' are transmitted to the smart card 10 and stored therein. Since the encrypted user certificate Cert' cannot be analyzed at the user side, necessary items such as an expiring time are transmitted in duplicate.

Although the first phase in a challenge-response authentication scheme has been described in detail, an authentication system according to the present invention can be achieved by a mutual authentication scheme wherein the user side and the network side authenticate each other.

Fig. 9 illustrates procedure in the first phase in the mutual-authentication mechanism. As shown in this figure, at first, an inherent card number IDu stored in this smart card 10 is read out and transmitted to the AuC 17 with a name of the application server APS NAME which will provide a desired network service as an authentication request. This transmission is represented by [IDu,APS NAME] in Fig. 9.

The AuC 17 generates a random number Rnd1 and transmits it to the smart card 10. The smart card 10 encrypts the received random number Rnd1 using the user secret key Ku stored in its memory to generate a response Res1 by means of a function Res1=f(Rnd1,Ku). The smart card 10 also generates a random number Rnd2. The generated response Res1 and the random number Rnd2 are transmitted to the AuC 17.

The AuC 17 inquires the user secret key Ku from the received card number IDu using the database 17a, and then, executes the same encryption of the random number Rnd1 as done in the smart card 10 using the user secret key Ku to generate Res1' by means of a function Res1'=f(Rnd1,Ku). The generated Res1' is then compared with the response Res1 transmitted from the smart card 10. If the user is a legitimate user and the user secret key Ku is correct one, Res1 will coincides with Res1'. However, if the user secret key Ku is incorrect, the calculated results Res1 and Res1' will not coincide with each other. In this case, failure of the authentication is informed to the user side and the process is terminated.

If the encrypted Res1' coincides with Res1, following procedure for authenticating the AuC 17 by the smart card 10 is carried out. First, the AuC 17 encrypts the random number Rnd2 transmitted from the smart card 10 using the user secret key Ku to generate a response Res2 by means of a function Res2=f(Rnd2,Ku). Then, the AuC 17 issues a user certificate Cert and an authentication information AuInfo for the smart card 10. Contents of the issued user certificate Cert and authentication information AuInfo are indicated in Fig. 11 as an example.

In order to prevent from fraudulent, the user certificate Cert is encrypted using a APS secret key Ka which is shared only by the AuC 17 and the APS 16 corresponding to the application server name APS NAME, to produce Cert'. Namely, by using a cryptographic function f, Cert' is obtained from Cert'=f(Cert,Ka). The response Res2, the authentication information AuInfo and the encrypted user certificate Cert' are transmitted to the smart card 10. Since the encrypted user certificate Cert' cannot be analyzed at the user side, necessary items such as an expiring time are transmitted in duplicate. The smart card 10 executes the same encryption of the random number Rnd2 as done in the AuC 17 using the user secret key Ku to generate Res2' by means of a function Res2'=f(Rnd2,Ku). The generated Res2' is then compared with the response Res2 transmitted from the AuC 17. If the AuC is a legitimate authentication center, Res2 will coincides with Res2'. Therefore, in this case, the encrypted user certificate Cert' and the authentication information AuInfo are stored in the memory in the smart card 10. However, if the calculated results Res2 and Res2' do not coincide with each other, it is judged that the AuC 17 is not legitimate one and thus the authentication is failed. In this case, the issued user certificate Cert' and authentication information AuInfo are canceled.

In order to protect the authentication information AuInfo and the user certificate Cert' from being eavesdropped and fraudulently accessed by a third party when they are transmitted from the AuC 17 to the smart card 10, the authentication information AuInfo and the user certificate Cert' may be encrypted by a session key shared by the AuC 17 and the smart card 10. It is desired to produce a session key in accordance with the random numbers Rnd1 and Rnd2 and the user secret key Ku shared only by the AuC 17 and the smart card 10.

Fig. 8 illustrates procedure in the second phase for requesting and enjoying a network service. As shown in this figure, at first, the encrypted user certificate Cert' which has been stored in the smart card 10 is read out and transmitted to the application server 16. This transmission is represented by [Cert'] in Fig. 8. It should be noted that the user certificate Cert' can be issued only by the AuC 17 and can be evaluated only by the application server 16, and that not only the smart card 10 but also the client terminal 12 cannot analyze it.

The application server 16 decrypts the transmitted user certificate Cert' using its APS secret key Ka to extract the original user certificate Cert. Then, the application server 16 evaluates or verifies the user certificate Cert by checking known or estimative information such as application server name, issuance time or validity time period contained in the certificate Cert. For example, if the certificate Cert is forged one, no significant information can be extracted there from and thus analysis of the certificate Cert fails. Even if the certificate Cert is legitimate one, this certificate Cert may be dealt with invalid when the validity time is expired.

Since the user certificate Cert' encrypted by using the APS secret key Ka is transmitted through the network when the smart card 10 accesses to the application server 16, a fraudulent third party may copies the encrypted certificate Cert' and may use it by stealth. In order to prevent such fraudulent usage, a challenge-response authentication is also executed between the smart card 10 and the application server 16. Namely, the application server 16 generates a random number Rnd and transmits it to the smart card 10. The smart card 10 encrypts the received random number Rnd using the user and APS shared key Ku-a contained in the authentication information sent from the AuC 17 when the user certificate was issued, to generate a response Res by means of a function Res=f(Rnd,Ku-a). The generated response Res is transmitted to the application server 16.

The application server 16 executes the same encryption of the random number Rnd as done in the smart card 10 using the user and APS shared key Ku-a which was contained in the decrypted used certificate Cert to generate Res' by means of a function Res'=f(Rnd,Ku-a). The generated Res' is then compared with the response Res transmitted from the smart card 10. If the user is a legitimate user, Res will coincides with Res'. However, if the user is a fraudulent user, the calculated results Res and Res' will not coincide with each other. In this case, although the certificate Cert is correct, it may be used by stealth. Thus, failure of the authentication is informed to the user side and the process is terminated.

If the encrypted Res' coincides with Res, the authentication is succeeded and the network service requested by the user is provided to the client terminal 12.

The user and APS shared key Ku-a is contained in both the user certificate and the authentication information sent from the AuC 17 to the smart card 10 during the accessing procedure to the AuC 17, shown in Figs. 7 and 9. This is also apparent from Fig. 11. Since the user certificate is decrypted only by the application server 16 having the APS secret key Ka and the authentication information is stored in the smart card 10 not stored in the application server 16, this user and APS shared key Ku-a is sent in duplicate. Even if a third party steals the user certificate encrypted by the APS secret key Ka, he cannot analyze it. Therefore, he cannot

encrypt the random number Rnd by using the user and APS shared key Ku-a.

Fig. 10 illustrates procedure in the second phase in the mutual authentication mechanism. As shown in this figure, at first, at first, the encrypted user certificate Cert' which has been stored in the smart card 10 is read out and transmitted to the application server 16. This transmission is represented by (Cert') in Fig. 10. It should be noted that the user certificate Cert' can be issued only by the AuC 17 and can be evaluated only by the application server 16, and that not only the smart card 10 but also the client terminal 12 cannot analyze it.

The application server 16 decrypts the transmitted user certificate Cert' using its APS secret key Ka to extract the original user certificate Cert. Then, the application server 16 evaluates or verifies the user certificate Cert by checking known or estimative information such as application server name, issuance time or validity time period contained in the certificate Cert. For example, if the certificate Cert is forged one, no significant information can be extracted there from and thus analysis of the certificate Cert fails. Even if the certificate Cert is legitimate one, this certificate Cert may be dealt with invalid when the validity time is expired.

Since the user certificate Cert' encrypted by using the APS secret key Ka is transmitted through the network when the smart card 10 accesses to the application server 16, a fraudulent third party may copies the encrypted certificate Cert' and may use it by stealth. In order to prevent such fraudulent usage, the mutual authentication is executed between the smart card 10 and the application server 16. Namely, the application server 16 generates a random number Rnd1 and transmits it to the smart card 10. The smart card 10 encrypts the received random number Rnd1 using the user and APS shared key Ku-a contained in the authentication information sent from the AuC 17 when the user certificate was issued, to generate a response Res by means of a function Res1=f(Rnd1,Ku-a). The smart card 10 also generates a random number Rnd2. The generated response Res1 and the random number Rnd2 are transmitted to the application server 16.

The application server 16 executes the same encryption of the random number Rnd as done in the smart card 10 using the user and APS shared key Ku-a which was contained in the decrypted used certificate Cert and extracted therefrom, to generate Res1' by means of a function Res1'=f(Rnd1,Ku-a). The generated Res1' is then compared with the response Res1 transmitted from the smart card 10. If the user is a legitimate user, Res1 will coincides with Res1'. However, if the user is a fraudulent user, the calculated results Res1 and Res1' will not coincide with each other. In this case, although the certificate Cert is correct, it may be used by stealth. Thus, failure of the authentication is informed to the user side and the process is terminated.

If the encrypted Res1' coincides with Res1, following procedure for authenticating the application server 16 by the smart card 10 is carried out. First, the application server 16 encrypts the random number Rnd2 transmitted from the smart card 10 using the user and APS shared key Ku-a to generate a response Res2 by means of a function Res2=f(Rnd2,Ku-a). Then, the generated Res2 is transmitted to the smart card 10.

The smart card 10 executes the same encryption of the random number Rnd2 as done in the application server 16 using the user and APS shared key Ku-a to generate Res2' by means of a function Res2'=f(Rnd2,Ku-a). The generated Res2' is then compared with the response Res2 transmitted from the application server 16. If the application server is a legitimate one, Res2 will coincides with Res2'. However, if the application server is an incorrect one, the calculated results Res2 and Res2' will not coincide with each other. In this case, failure of the authentication is informed to the user and the process is terminated.

If the encrypted Res2' coincides with Res2, the mutual authentication is succeeded and the network service requested by the user is provided to the client terminal 12.

In this second embodiment, it is important that the user certificate which can be used for one or more times is securely stored without being stolen by a third party. For this purpose, it is effective to execute cryptographic function within an IC card provided with a CPU (smart card) which can subjectively manage accesses and to store a user certificate in the card.

As is described in detail, according to the present invention, an authentication system adopting an authentication scheme for verifying a user from a network, by sharing the same secret key between the user and the network, encrypting a known information using the secret key at the user to produce first encrypted information, transmitting the first encrypted information from the user to the network, encrypting the known information using the secret key at the network to produce second encrypted information, and collating the transmitted first encrypted information with the produced second encrypted information at the network, has system comprising a single master authentication center arranged in the network, the master authentication center sharing with the user a user secret key, and a plurality of slave authentication centers sharing with the master authentication center respective secret keys different from the user secret key. The master authentication center authenticates the user by using the user secret key and issues a certificate information which certifies legitimation of the user, to the user if the user is authenticated as a legitimate user. The slave authentication center authenticates the certificate information from the user and issues a permission information which allows an access to a specified server or an application server in the network, to the user if the user is authenticated as a legitimate user.

Therefore, in case of verifying a user by presenting a calculation result of the user's inherent information, authentication processes can be executed by distributed servers in the network without sharing user's

secret information. In other words, according to the present invention, by using a user certificate which is valid for a predetermined period or predetermined times, authentication processes can be executed by distributed servers in the network without sharing user's secret information. A part of authentication load can be shared by application servers instead of slave authentication centers.

In near future, decisions or purchases and sales via a wide range network such as Internet or CATV network will greatly increase, and therefore requests of user authentications via a plurality of networks or within a single network will extremely increase. According to the present invention, a very effective authentication system can be provided under these circumstances.

Many widely different embodiments of the present invention may be constructed without departing from the spirit and scope of the present invention. It should be understood that the present invention is not limited to the specific embodiments described in the specification, except as defined in the appended claims.

Claims

1. An authentication system adopting an authentication scheme for verifying a user from a network, by sharing the same secret key between the user and the network, encrypting a known information using said secret key at the user to produce first encrypted information, transmitting the first encrypted information from the user to the network, encrypting the known information using said secret key at the network to produce second encrypted information, and collating the transmitted first encrypted information with the produced second encrypted information at the network,

   said system comprising a single master authentication center arranged in the network, said master authentication center sharing with the user a user secret key, and a plurality of slave authentication centers sharing with said master authentication center respective secret keys different from the user secret key,

   said master authentication center authenticating the user by using said user secret key and issuing a certificate information to the user if the user is authenticated as a legitimate user, said certificate information certifying legitimation of the user, said slave authentication center authenticating the certificate information from the user and issuing a permission information which allows an access to a specified server or an application server in the network, to the user if the user is authenticated as a legitimate user.

2. The authentication system as claimed in claim 1, wherein said system adopts a mutual authentication scheme for further verifying the network from the user, by encrypting a known information using said secret key at the network to produce third encrypted information, transmitting the third encrypted information from the network to the user, encrypting the known information using said secret key at the user to produce fourth encrypted information, and collating the transmitted third encrypted information with the produced fourth encrypted information at the user.

3. The authentication system as claimed in claim 1, wherein said user has an IC card provided with a CPU, and wherein the IC card executes management of said user secret key and encryption and decryption of the information.

4. The authentication system as claimed in claim 1, wherein said secret key used for encrypting the known information is one using a random number generated at the user.

5. An authentication system adopting an authentication scheme for verifying a user from a network, by sharing the same secret key between the user and the network, encrypting a known information using said secret key at the user to produce first encrypted information, transmitting the first encrypted information from the user to the network, encrypting the known information using said secret key at the network to produce second encrypted information, and collating the transmitted first encrypted information with the produced second encrypted information at the network,

   said network issuing a certificate information to the user if the user is authenticated as a legitimate user, said certificate information certifying legitimation of the user and being valid within a predetermined period or predetermined times.

6. The authentication system as claimed in claim 5, wherein said user has an IC card provided with a CPU, and wherein the IC card executes management of said user secret key, management of the certificate information issued at the network, and encryption and decryption of the information.

7. The authentication system as claimed in claim 5, wherein said system adopts a mutual authentication scheme for further verifying the network from the user, by encrypting a known information using said secret key at the network to produce third encrypted information, transmitting the third encrypted information from the network to the user, encrypting the known information using said secret key at the user to produce fourth encrypted information, and collating the transmitted third encrypted information with the produced fourth encrypted information at the user.

Fig. 1

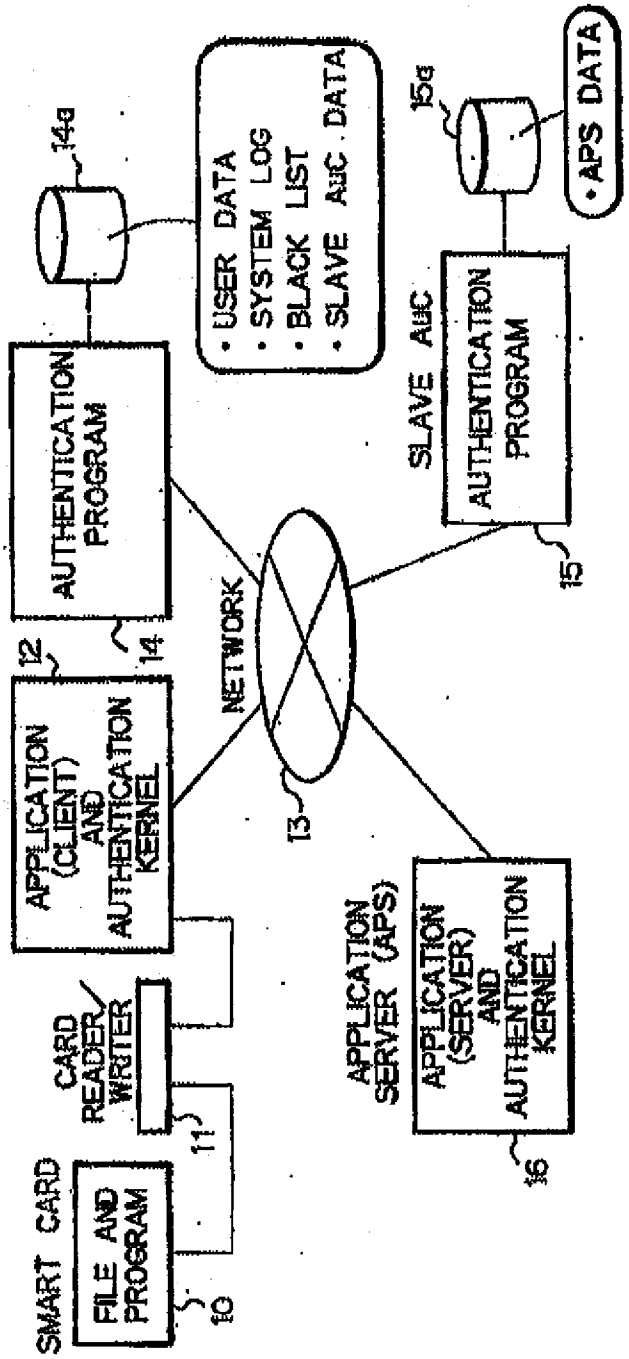

CLIENT TERMINAL
APPLICATION (CLIENT) AND AUTHENTICATION KERNEL
12
MASTER AuC
AUTHENTICATION PROGRAM
14
14a
• USER DATA
• SYSTEM LOG
• BLACK LIST
• SLAVE AuC DATA
NETWORK
13
SLAVE AuC
AUTHENTICATION PROGRAM
15
15a
• APS DATA
CARD READER WRITER
11
SMART CARD
FILE AND PROGRAM
10
APPLICATION SERVER (APS)
APPLICATION (SERVER) AND AUTHENTICATION KERNEL
16

Fig. 2

① REQUEST AND ISSUANCE OF USER CERTIFICATE
② REQUEST AND ISSUANCE OF SERVICE UTILIZATION PERMISSION
③ REQUEST AND ENJOYMENT OF NETWORK SERVICE

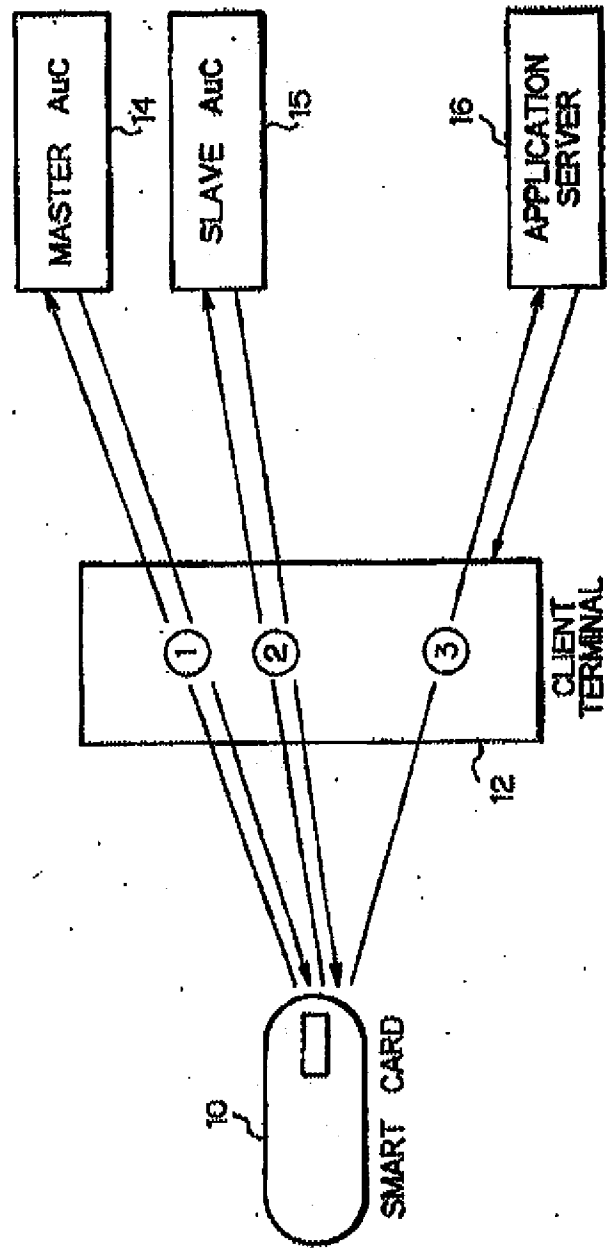


Fig. 3

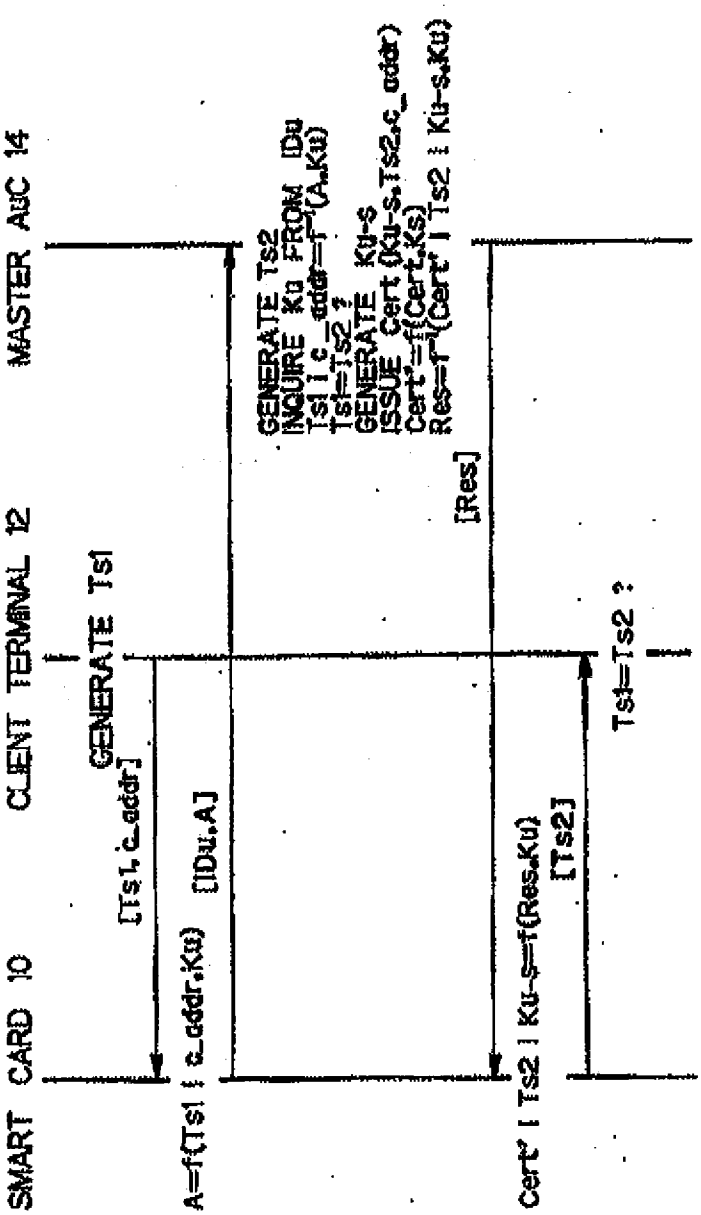

SMART CARD 10
CLIENT TERMINAL 12
MASTER A&C 14
GENERATE Ts1
[Ts1, c_addr]
A=f(Ts1 | c_addr,Ku)
[IDu, A]
GENERATE Ts2
INQUIRE Ku FROM IDu
Ts1 | c_addr=f⁻¹(A,Ku)
Ts=Ts2 ?
GENERATE Ku-s
ISSUE Cert (Ku-s,Ts2,c_addr)
Cert'=f(Cert,Ks)
Res=f⁻¹(Cert' | Ts2 | Ku-s,Ku)
[Res]
Cert' | Ts2 | Ku-s=f(Res,Ku)
[Ts2]
Ts1=Ts2 ?

Fig. 4

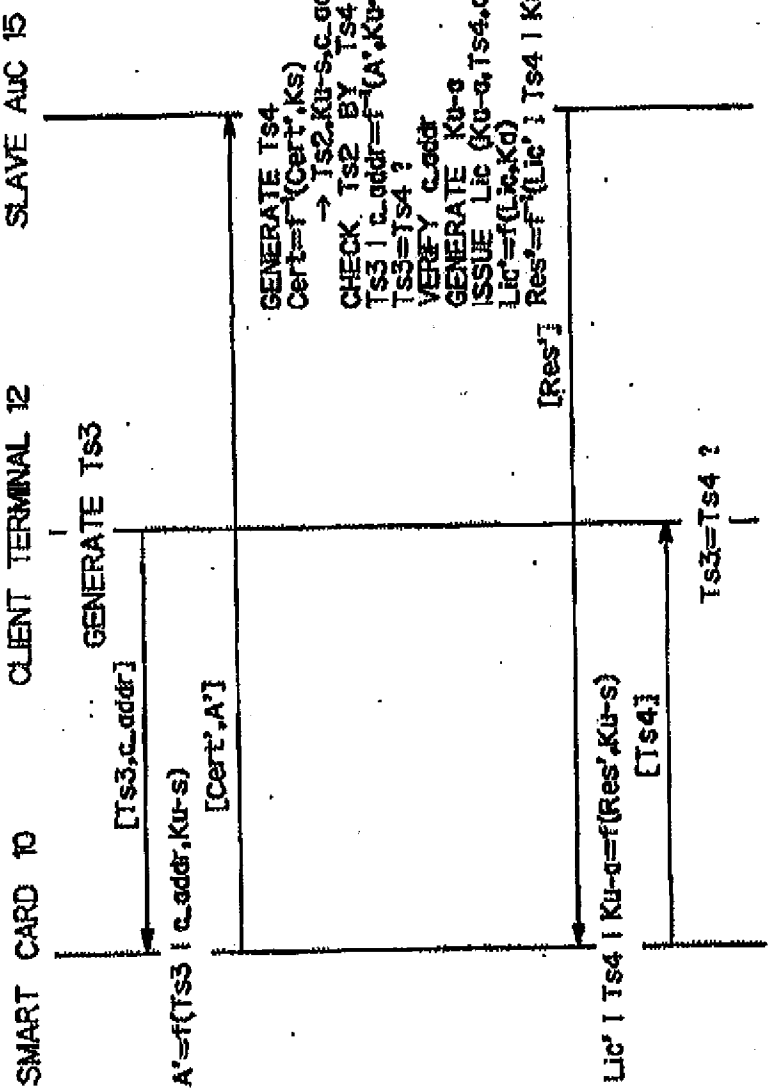

SMART CARD 10
CLIENT TERMINAL 12
SLAVE AUC 15
GENERATE Ts3
[Ts3,c_addr]
A'=f(Ts3 | c_addr,Ku-s)
[Cert',A']
GENERATE Ts4
Cert'=f'(Cert',Ks)
→ Ts2,Ku-s,c_addr
CHECK Ts2 BY Ts4
Ts3 | c_addr=f'(A',Ku-s)
Ts3=Ts4 ?
VERIFY c_addr
GENERATE Ku-s
ISSUE Lic (Ku-s, Ts4,c_addr)
Lic'=f(Lic,Kd)
Res'=f'(Lic' | Ts4 | Ku-s,Ku-s)
[Res']
Lic' | Ts4 | Ku-s=f(Res',Ku-s)
[Ts4]
Ts3=Ts4 ?

Fig. 5

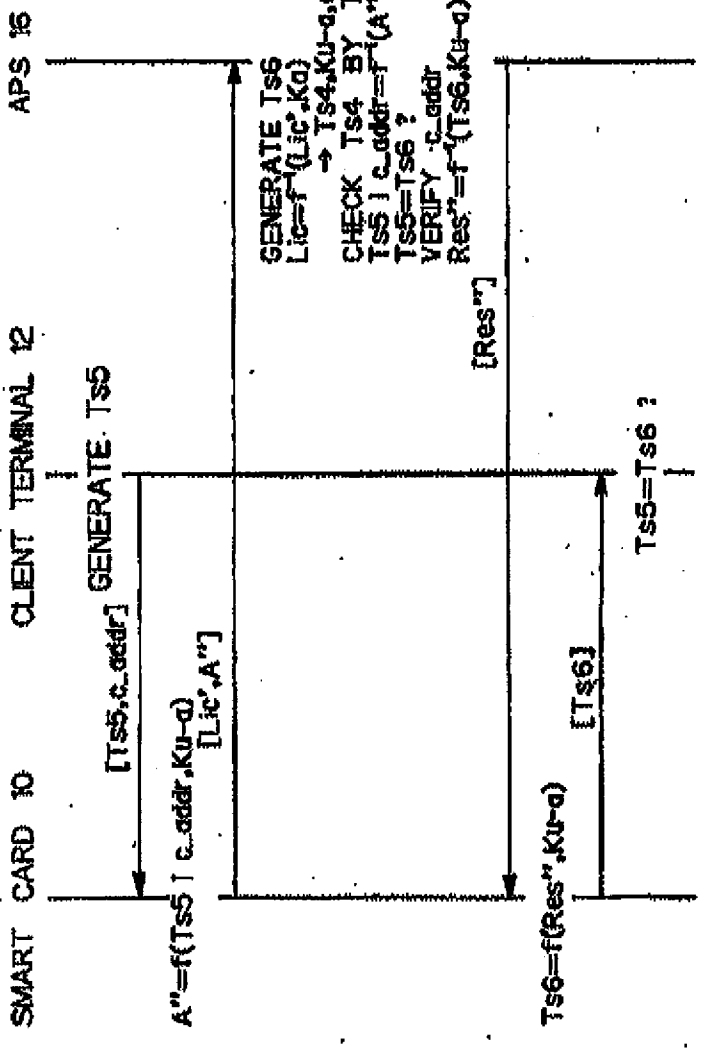

SMART CARD 10
CLIENT TERMINAL 12
APS 16
GENERATE Ts5
[Ts5,c_addr]
A''=f(Ts5 | c_addr,Ku-a)
[Lic',A'']
GENERATE Ts6
Lic=f(Lic',Ka)
→ Ts4,Ku-a,c_addr
CHECK Ts4 BY Ts6
Ts5 | c_addr=f(A'',Ku-a)
Ts5=Ts6 ?
VERIFY c_addr
Res''=f(Ts6,Ku-a)
[Res'']
Ts6=f(Res'',Ku-a)
[Ts6]
Ts5=Ts6 ?

Fig. 6

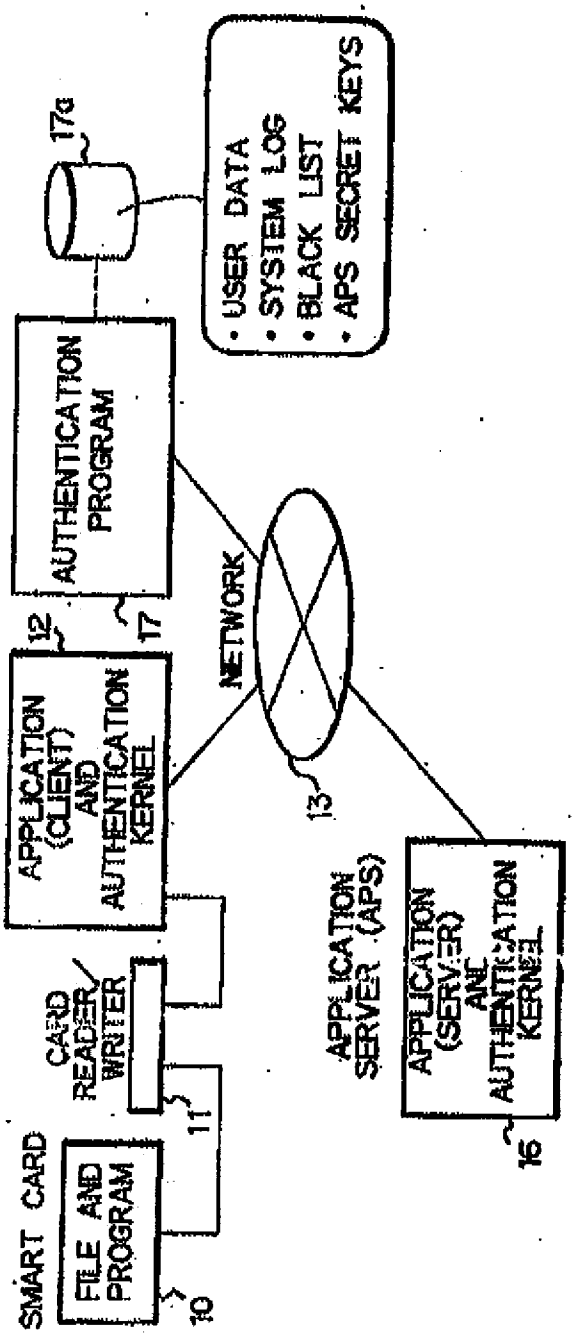

AuC
AUTHENTICATION PROGRAM
17
17a
• USER DATA
• SYSTEM LOG
• BLACK LIST
• APS SECRET KEYS
NETWORK
13
CLIENT TERMINAL
APPLICATION (CLIENT) AND AUTHENTICATION KERNEL
12
CARD READER/ WRITER
11
SMART CARD
FILE AND PROGRAM
10
APPLICATION SERVER (APS)
APPLICATION (SERVER) AND AUTHENTICATION KERNEL
16

Fig. 7

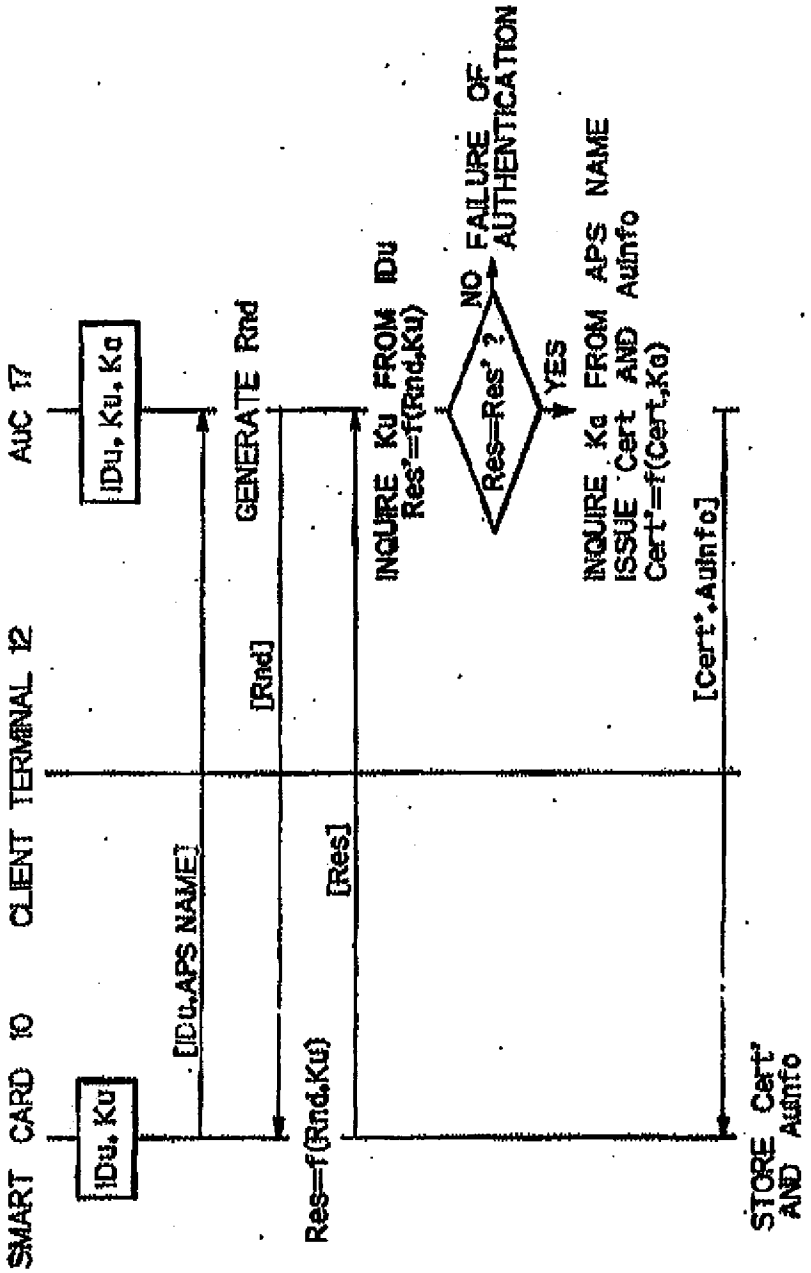
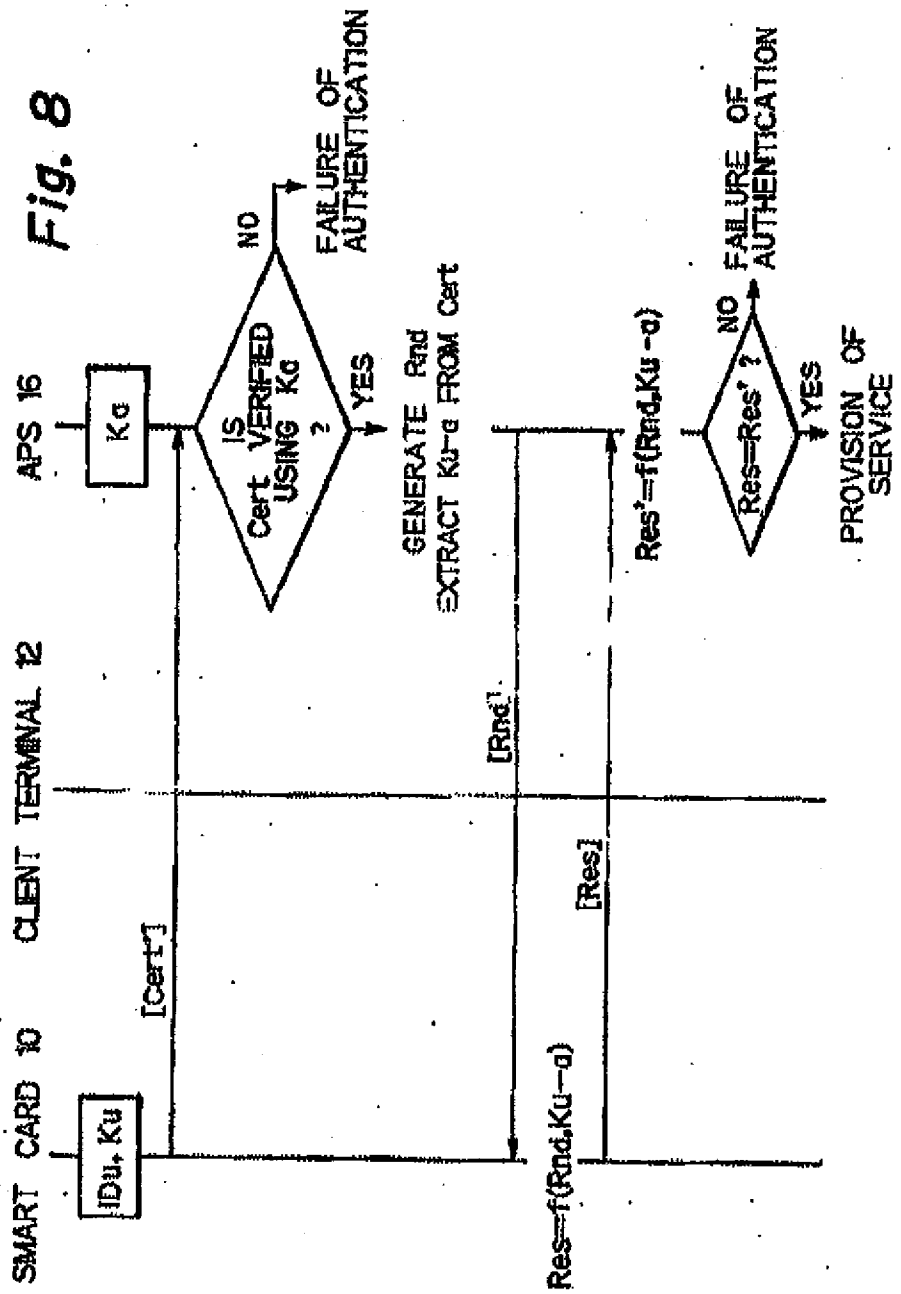

SMART CARD 10
CLIENT TERMINAL 12
AUC 17
IDu, Ku
IDu, Ku, Ka
[IDu,APS NAME]
GENERATE Rnd
[Rnd]
Res=f(Rnd,Ku)
[Res]
INQUIRE Ku FROM IDu
Res'=f(Rnd,Ku)
Res=Res' ?
NO
FAILURE OF AUTHENTICATION
YES
INQUIRE Ka FROM APS NAME
ISSUE Cert AND Authfo
Cert'=f(Cert,Ka)
[Cert',Authfo]
STORE Cert' AND Authfo

Fig. 8


SMART CARD 10
CLIENT TERMINAL 12
APS 16
IDu, Ku
Kα
[Cert']
IS Cert VERIFIED USING Kα ?
NO
FAILURE OF AUTHENTICATION
YES
GENERATE Rnd
EXTRACT Ku-α FROM Cert
[Rnd']
Res=f(Rnd,Ku−α)
[Res]
Res'=f(Rnd,Ku−α)
Res=Res' ?
NO
FAILURE OF AUTHENTICATION
YES
PROVISION OF SERVICE

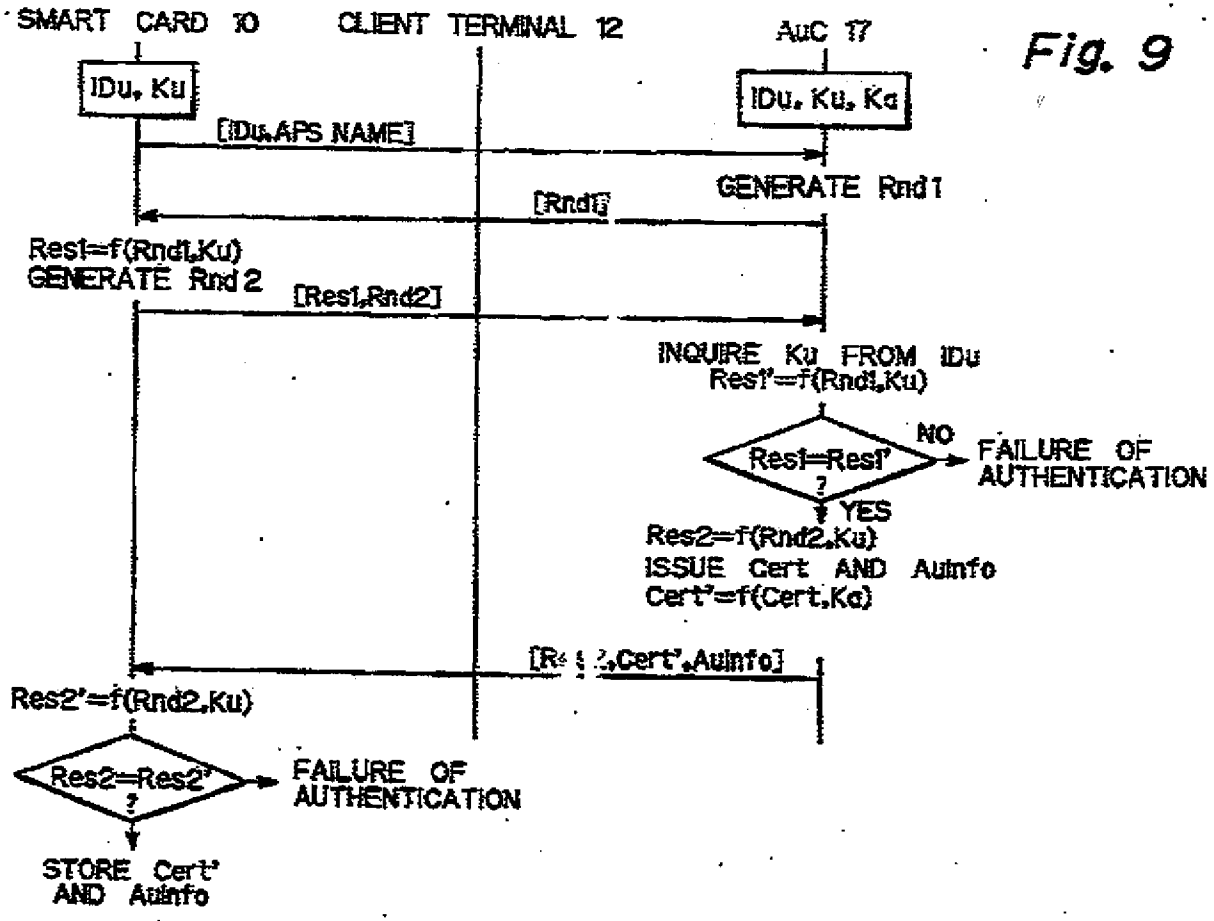


Fig. 9

EP 0 727 894 A1

Fig. 10

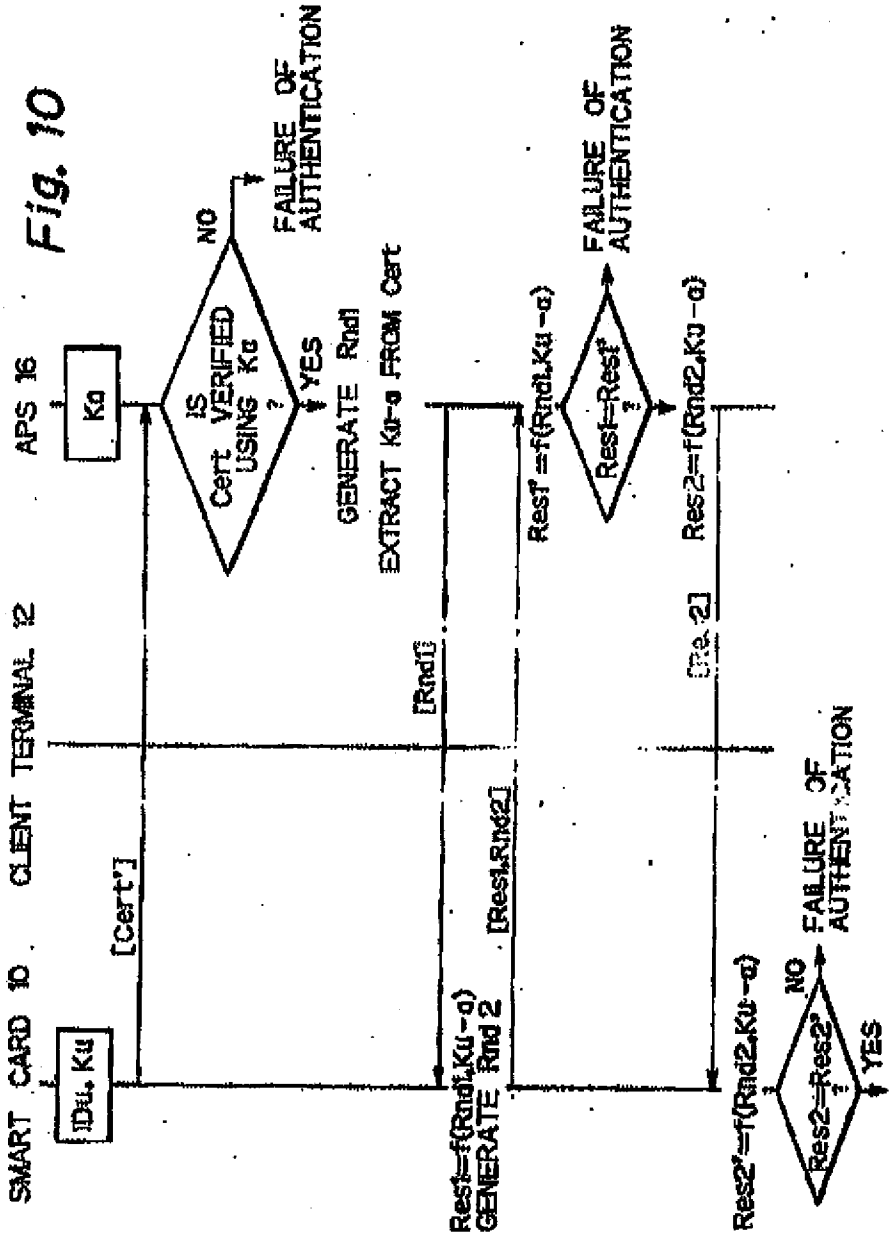
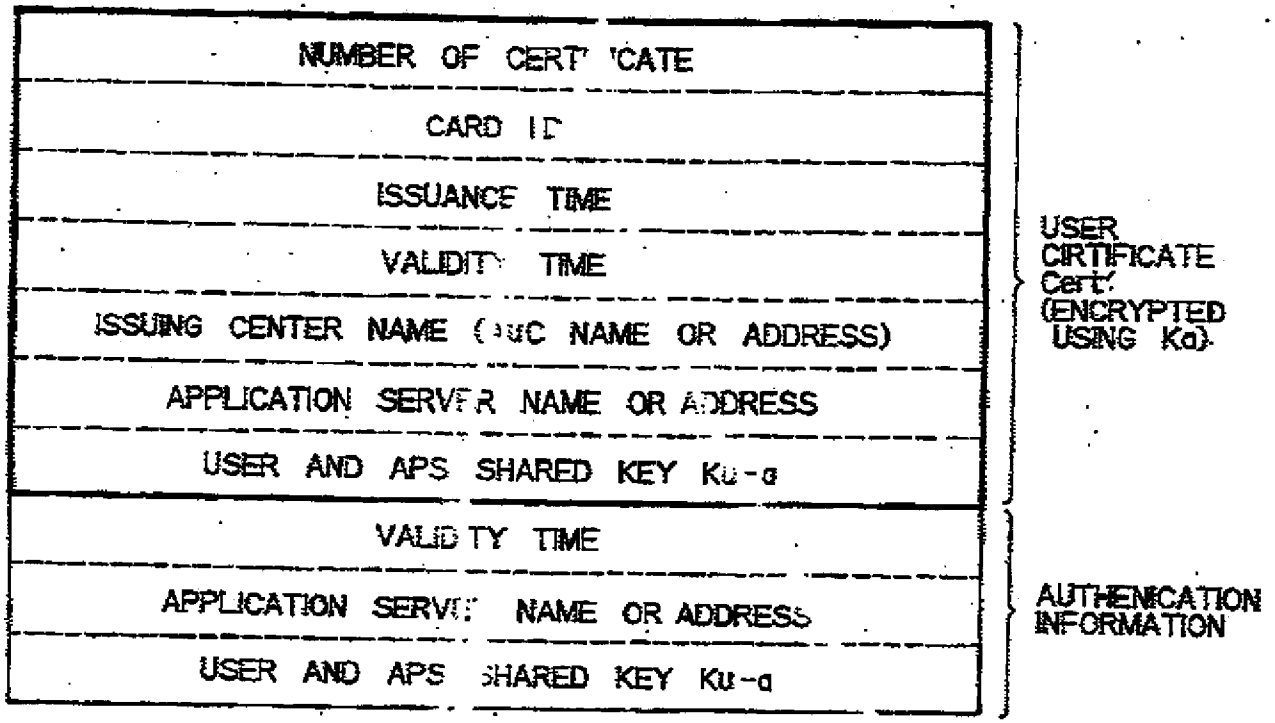

SMART CARD 10
CLENT TERMINAL 12
APS 16
IDu, Ku
Ka
[Cert']
IS Cert VERIFIED USING Ka ?
NO
FAILURE OF AUTHENTICATION
YES
GENERATE Rnd1
EXTRACT Ku-a FROM Cert
[Rnd1]
Res1=f(Rnd1,Ku-a)
GENERATE Rnd 2
[Res1,Rnd2]
Res1'=f(Rnd1,Ku-a)
Res1=Res1' ?
FAILURE OF AUTHENTICATION
[Rnd2]
Res2=f(Rnd2,Ku-a)
Res2'=f(Rnd2,Ku-a)
Res2=Res2' ?
NO
FAILURE OF AUTHENTICATION
YES

Fig. 11



EP 0 727 894 A1